ITA1466-ETHICAL HACKING

LAB MANUAL

Exercise No 1: Nmap Scan

NAME : M Mani Sai
Reg No : 192111399

Aim:

To install and perform Nmap scan (note :- you may use ip address or website name)

Procedure:

Step 1: Open Nmap from Kali Linux (Goto Applications->select Information Gathering->select Nmap)

Step 2: Perform different types of scan
(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

Scanning Techniques

Flag	Use	Example
-sS	**TCP syn port scan**	**nmap -sS 192.168.1.1**
-sT	**TCP connect port scan**	**nmap -sT 192.168.1.1**
–sU	**UDP port scan**	**nmap –sU 192.168.1.1**
–sA	**TCP ack port scan**	**nmap –sA 192.168.1.1**

Step 3:-
To perform host discovery

-Pn	only port scan	nmap -Pn192.168.1.1
-sn	only host discover	nmap -sn192.168.1.1
-PR	arp discovery on a local network	nmap -PR192.168.1.1
-n	disable DNS resolution	nmap -n 192.168.1.1

Step4:-

Port Specification

Flag	Use	Example
-p	**specify a port or port range**	**nmap -p 1-30 192.168.1.1**
-p-	**scan all ports**	**nmap -p- 192.168.1.1**
F	**fast port scan**	**nmap -F 192.168.1.1**

Step 5:-

Service Version and OS Detection

Flag	Use	Example
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1

Step 6:-

Timing and Performance

Flag	Use	Example
-T0	paranoid IDS evasion	nmap -T0 192.168.1.1
-T1	sneaky IDS evasion	nmap -T1 192.168.1.1
-T2	polite IDS evasion	nmap -T2 192.168.1.1
-T3	normal IDS evasion	nmap -T3 192.168.1.1

-T4	aggressive speed scan	nmap -T4 192.168.1.1
-T5	insane speed scan	nmap -T5 192.168.1.1

Output:

Step 1: Open Nmap from Kali Linux (Goto Applications->select Information Gathering->select Nmap)

Step 2: Perform different types of scan

(Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types

```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 13:48 IST
Nmap scan report for 192.168.1.1
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.38 seconds

┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 13:48 IST
Nmap scan report for 192.168.1.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 25.39 seconds

┌──(root㉿kali)-[~]
└─# nmap -sU 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 13:49 IST
Stats: 0:02:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 29.25% done; ETC: 13:57 (0:05:17 remaining)
Stats: 0:06:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.75% done; ETC: 14:05 (0:09:01 remaining)
Stats: 0:06:13 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.80% done; ETC: 14:05 (0:09:01 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.00090s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1719.23 seconds

┌──(root㉿kali)-[~]
└─# nmap -sA 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 13:51 IST
Nmap scan report for 192.168.56.1
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

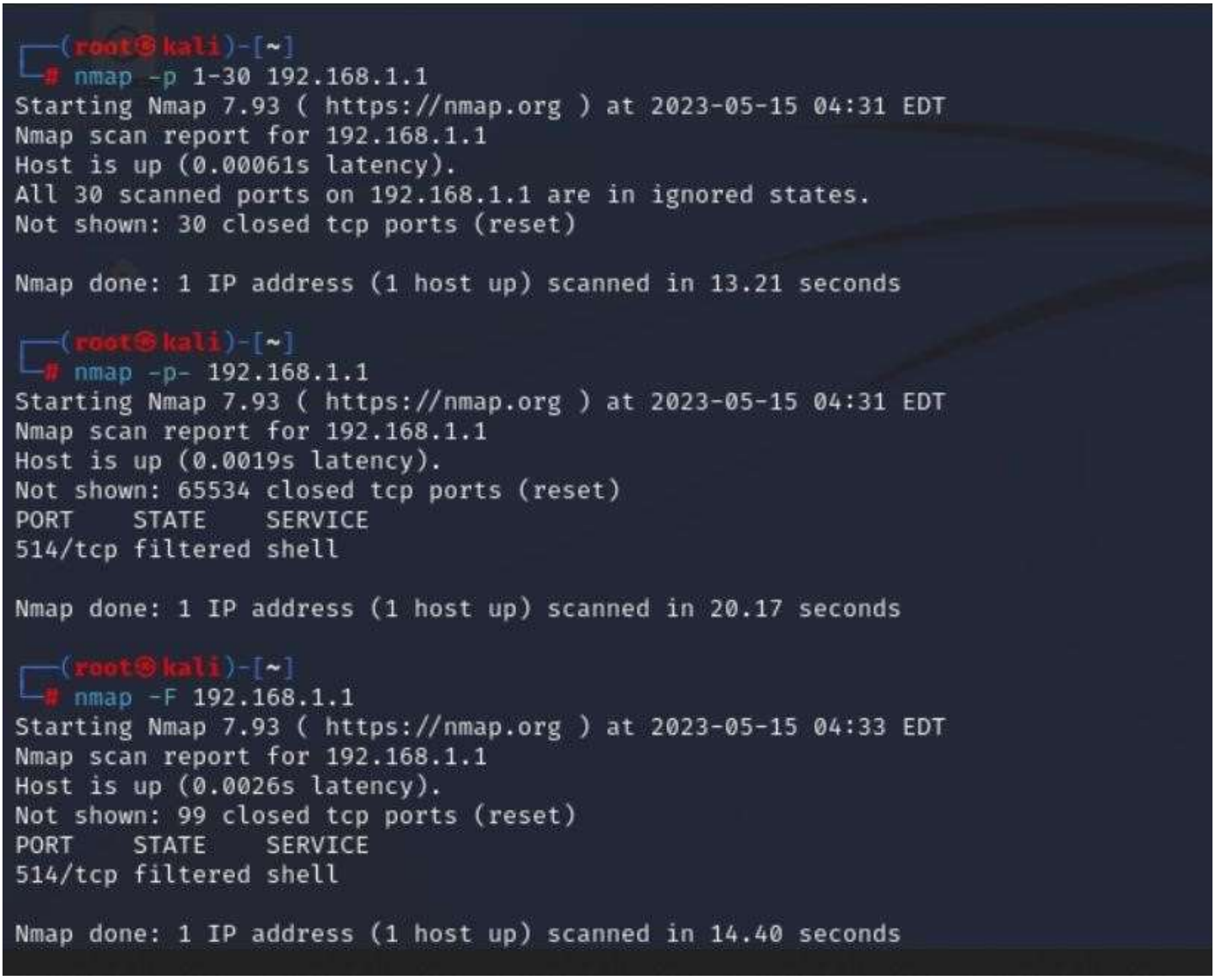
Step 3:-

To perform host discovery

```
┌──(root㉿kali)-[~]
└─# nmap -Pn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:24 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00098s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 14.42 seconds

┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:26 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00074s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds

┌──(root㉿kali)-[~]
└─# nmap -PR 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:26 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 14.49 seconds

┌──(root㉿kali)-[~]
└─# nmap -n 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:28 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0021s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

Step4:-

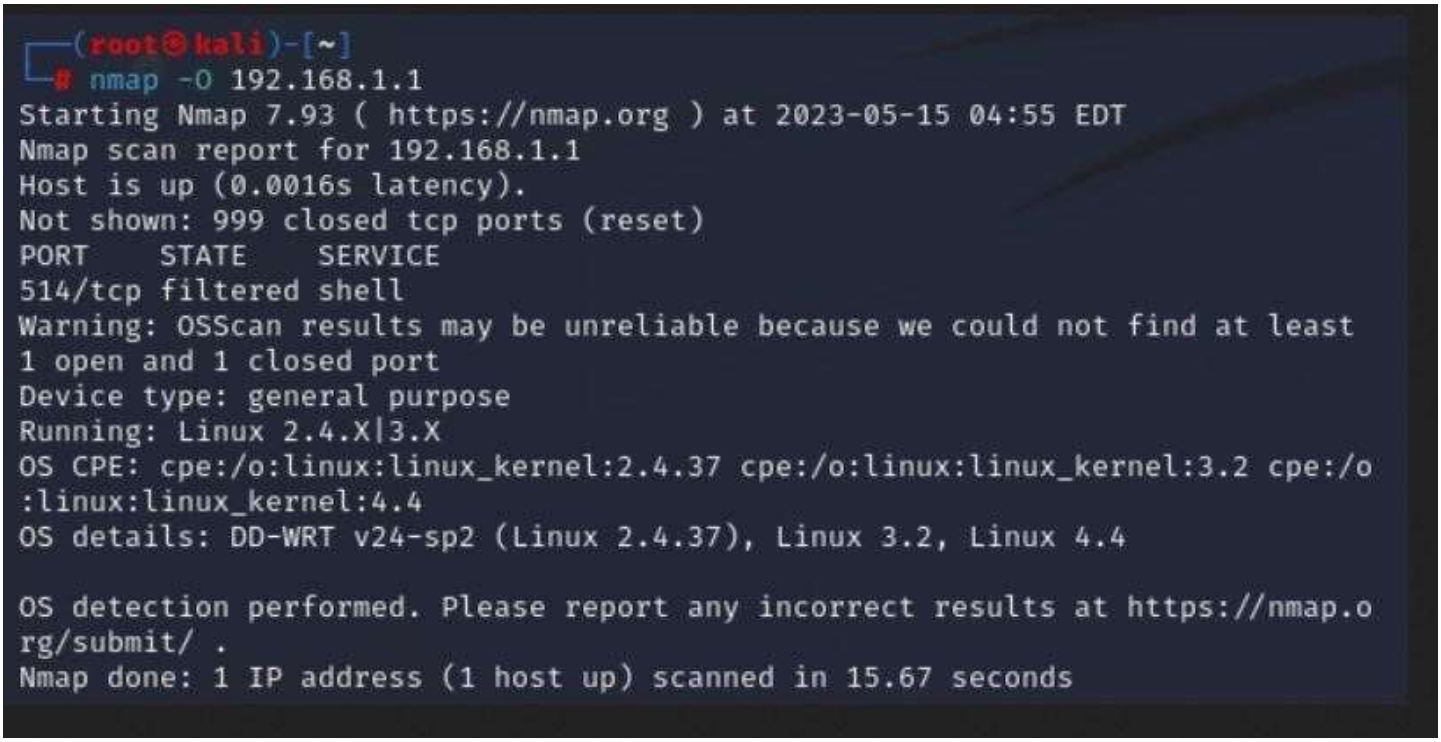
Port Specification



Step 5:-

Service Version and OS Detection

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:54 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE VERSION
514/tcp filtered shell

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds

┌──(root㉿kali)-[~]
└─# nmap -A 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 04:54 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE VERSION
514/tcp filtered shell
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o
:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.77 ms 192.168.50.2
2   1.25 ms 192.168.1.1

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.22 seconds
```

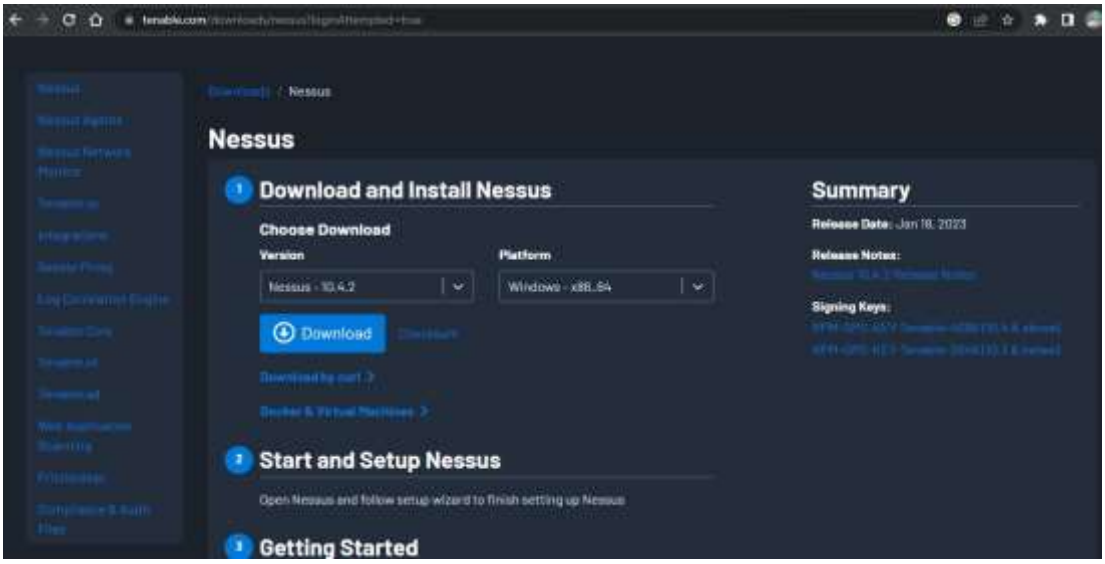


Result:

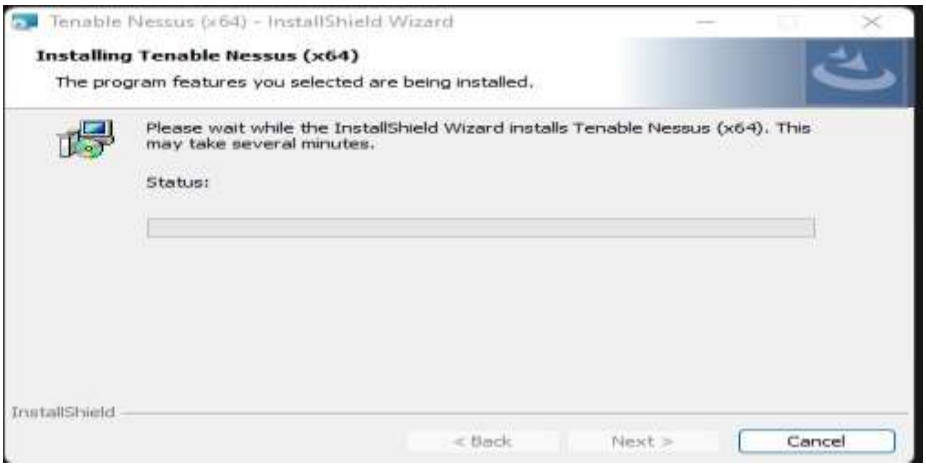
Exercise No 2: Vulnerability Access Scan Using Nessus

Aim : To Download and install Nessus tool and perform a Vulnerability Access scan in kali Linux Operating systems.

Step 1:- https://www.tenable.com/downloads/nessus?loginAttempted=true

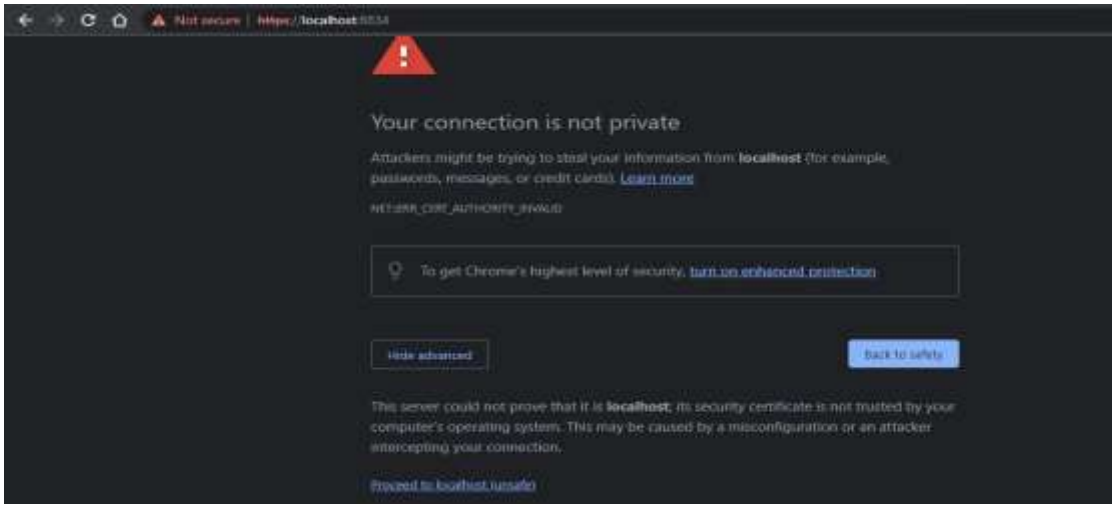


Step 2: Choose your OS and download , install



Step 3: Once installation is completed it will open in default browser

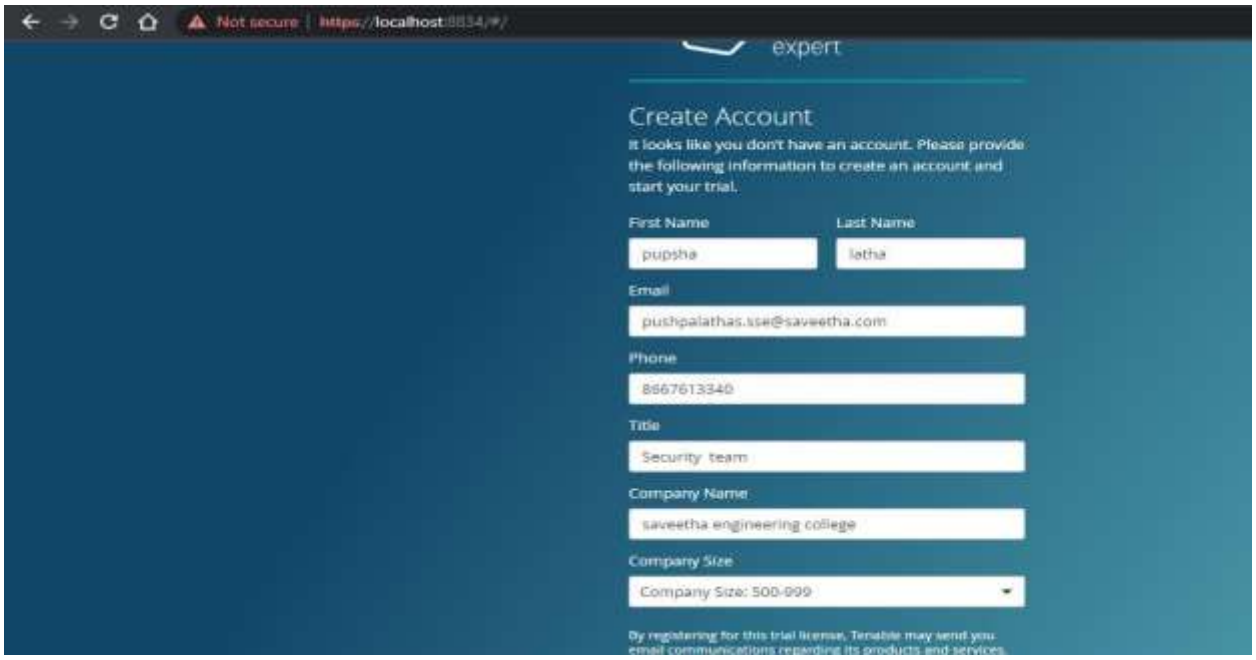
Step 5:- (click on the proceed to local host)



Step 6:- Please choose the Nessus Expert

Step 7: Click on continue

Step 8:- Register with your organizational email id

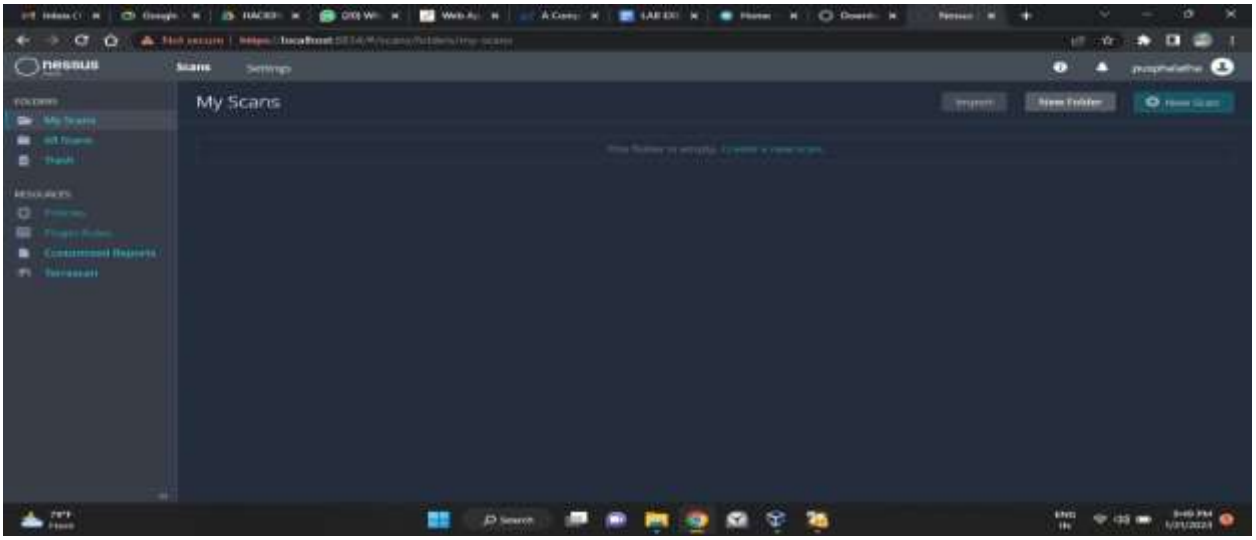


Step 9:- please note down the activation key

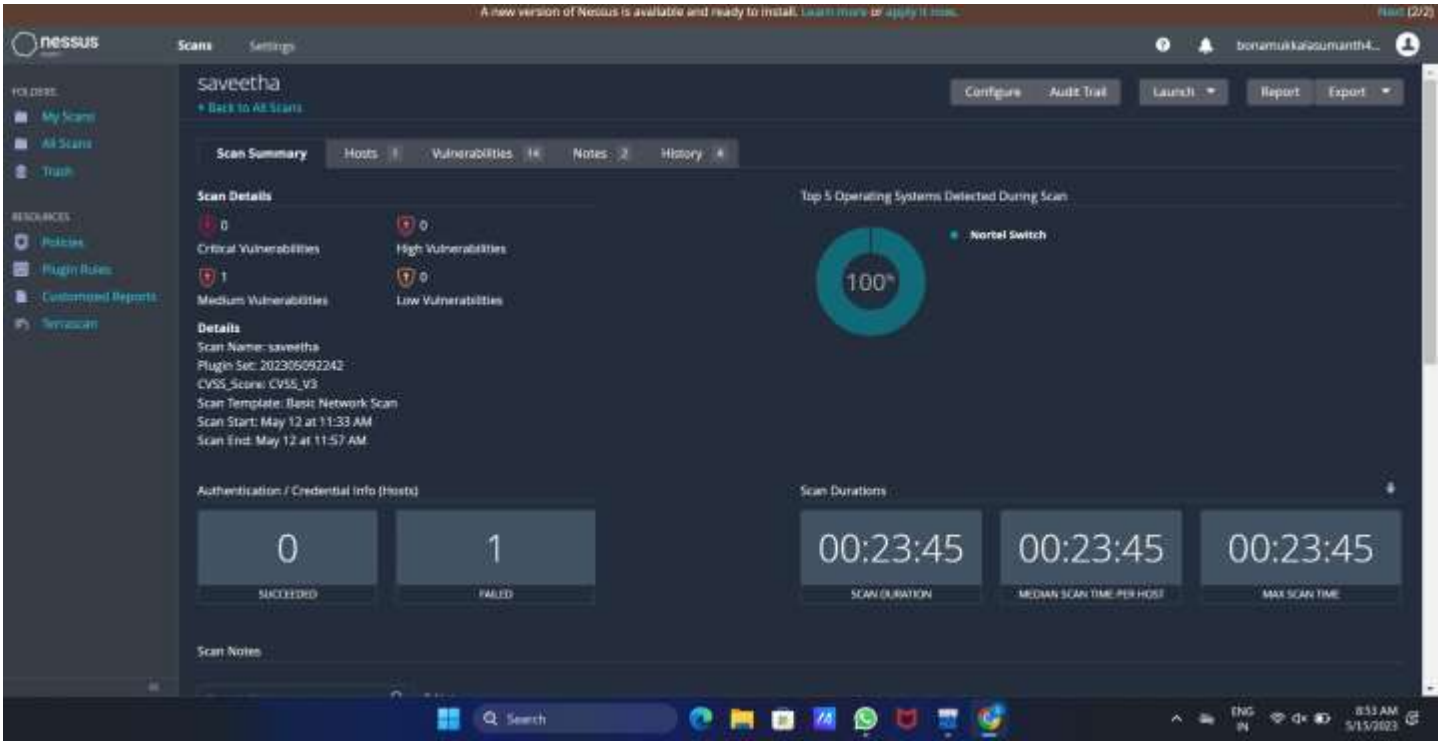
Step 10:- set up your username & password

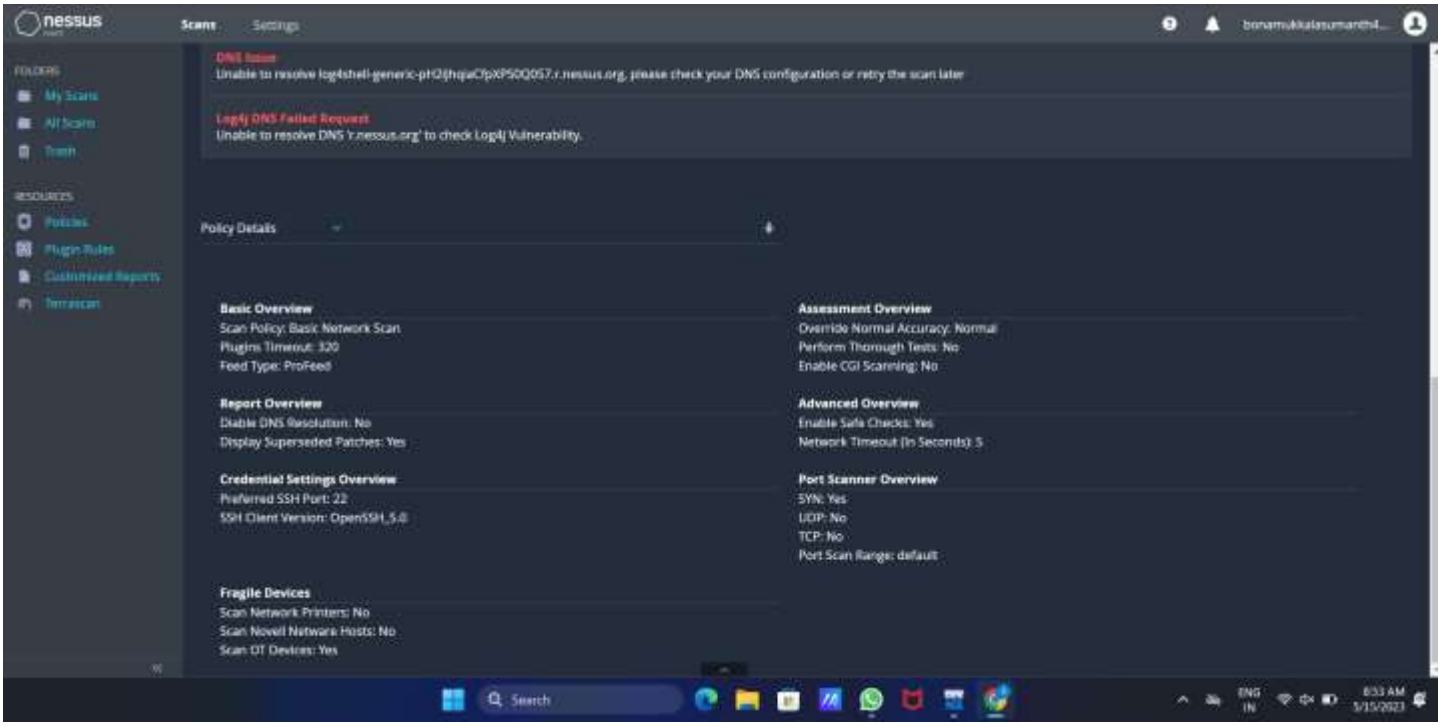
Step 11:-Type username and password

Step 12:- Please wait until download is completed


nessus
Scans
Settings
My Scans

Out Put:


A new version of Nessus is available and ready to install.
nessus
Scans
Settings
saveetha
Back to All Scans
Configure
Audit Trail
Launch
Report
Export
Scan Summary
Hosts 1
Vulnerabilities 14
Notes 2
History 4
Scan Details
0
Critical Vulnerabilities
0
High Vulnerabilities
1
Medium Vulnerabilities
0
Low Vulnerabilities
Details
Scan Name: saveetha
Plugin Set: 202305092242
CVSS_Score: CVSS_V3
Scan Template: Basic Network Scan
Scan Start: May 12 at 11:33 AM
Scan End: May 12 at 11:57 AM
Top 5 Operating Systems Detected During Scan
Nortel Switch
100%
Authentication / Credential Info (Hosts)
0
SUCCEEDED
1
FAILED
Scan Durations
00:23:45
SCAN DURATION
00:23:45
MEDIAN SCAN TIME PER HOST
00:23:45
MAX SCAN TIME
Scan Notes
Search



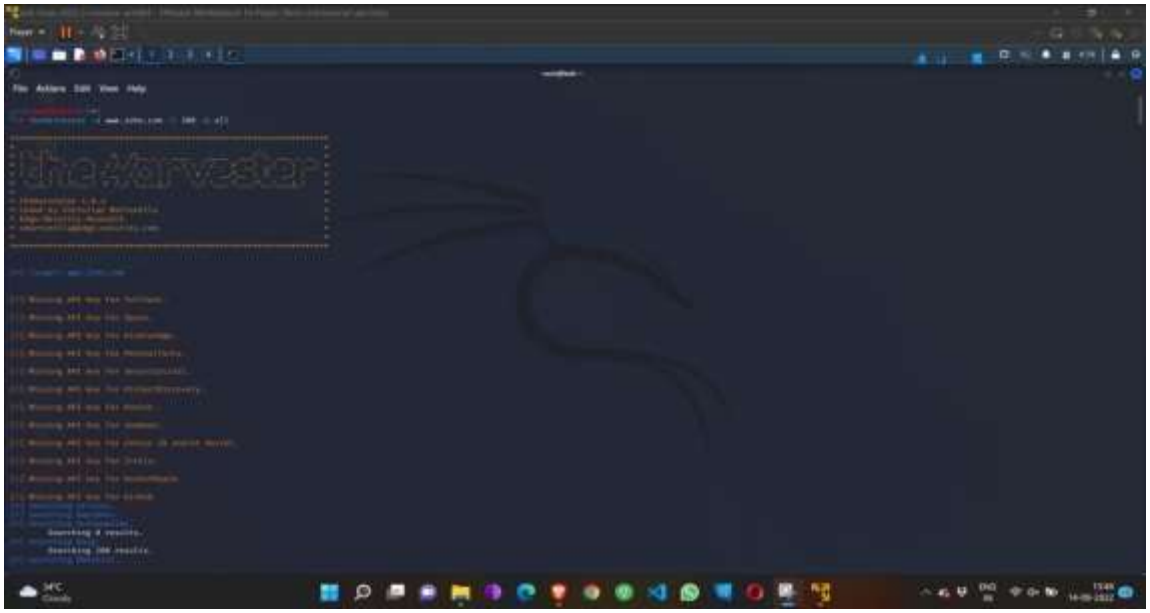
Exercise No 3: Information gathering using theHarvester

Aim: To demonstrate information gathering using theHarvester **Procedure:**

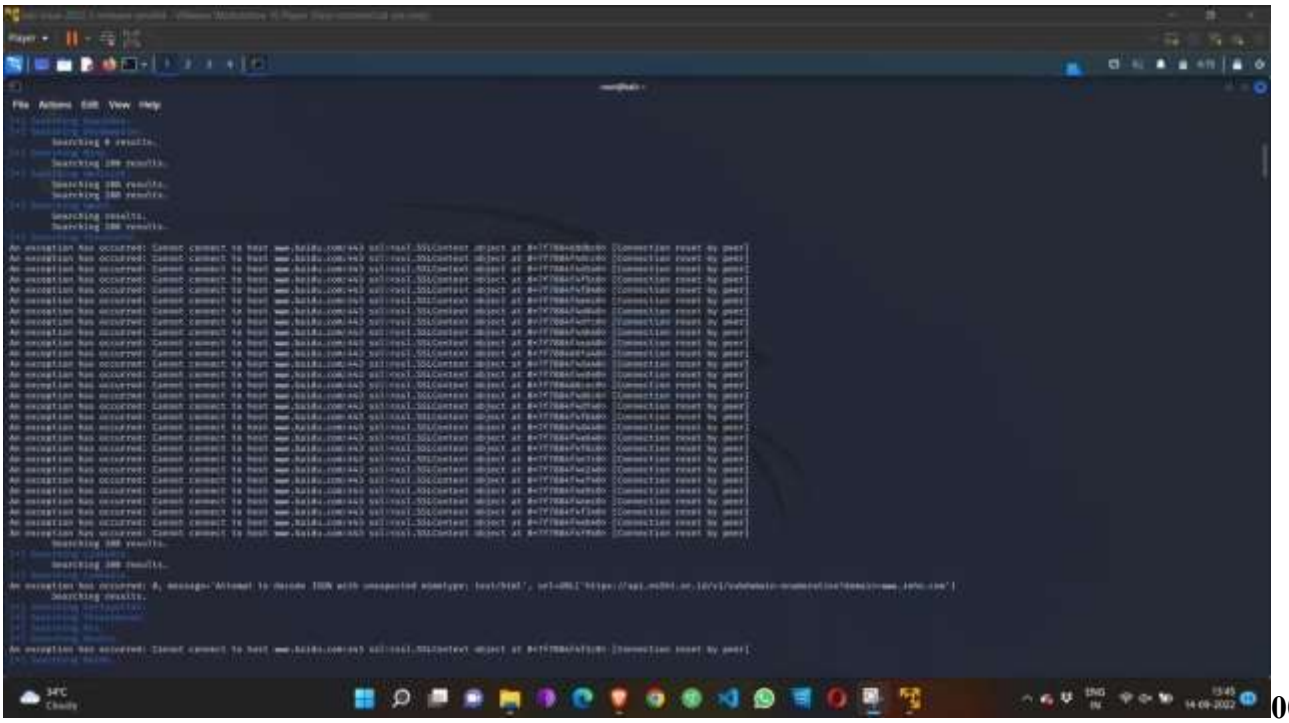
STEP 1: Open Terminal in the kali linux

```
-d [url] will be the remote site from which you wants to fetch


-l will limit the search for specified number.

-b is used to specify search engine name.
```

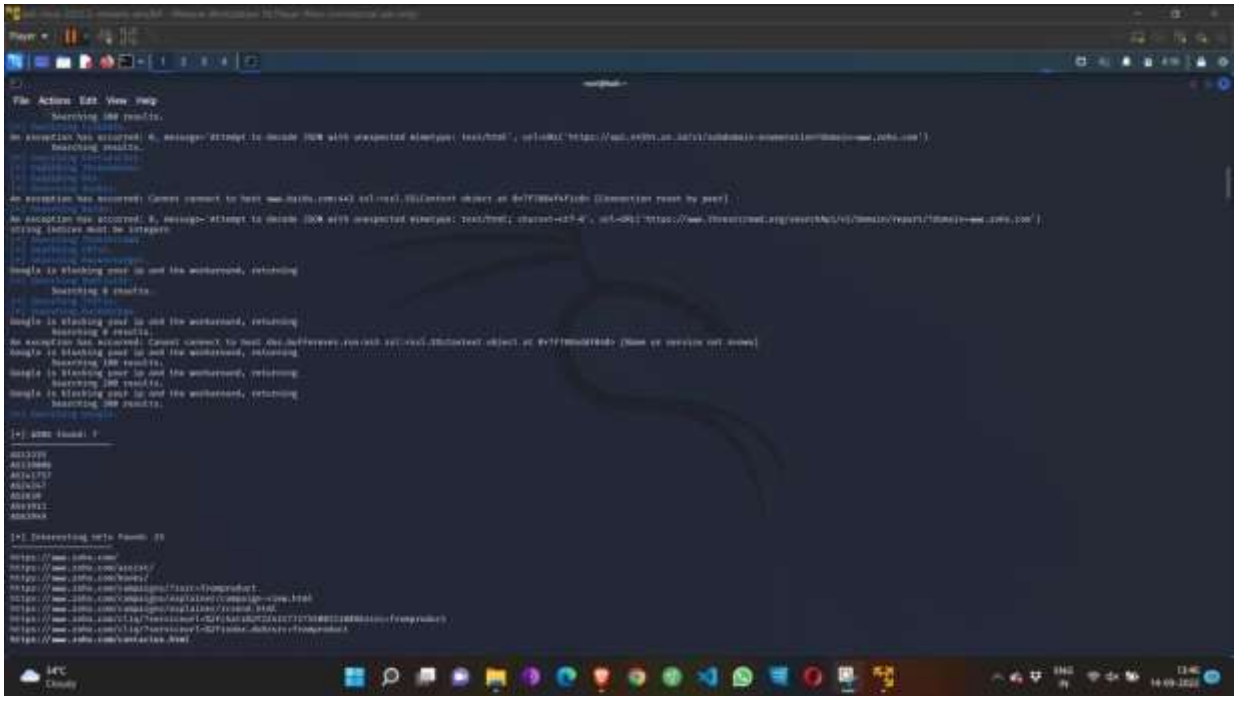
STEP 2: Run the following command

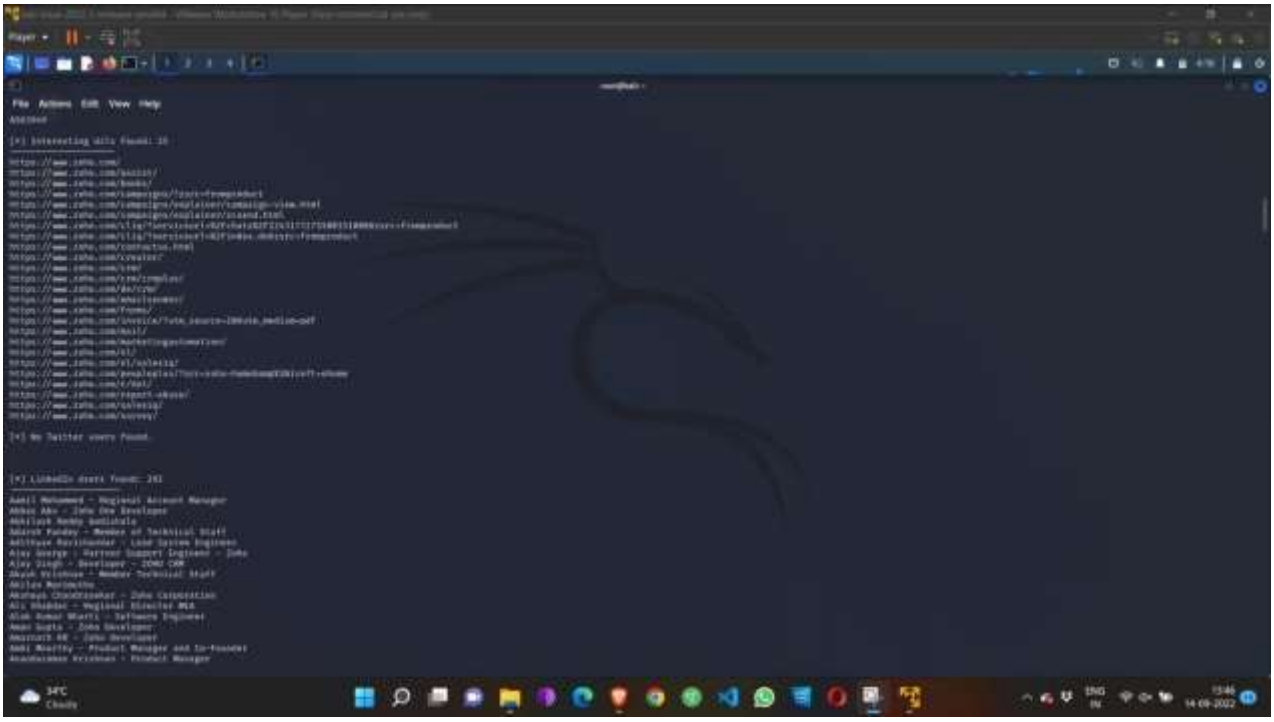


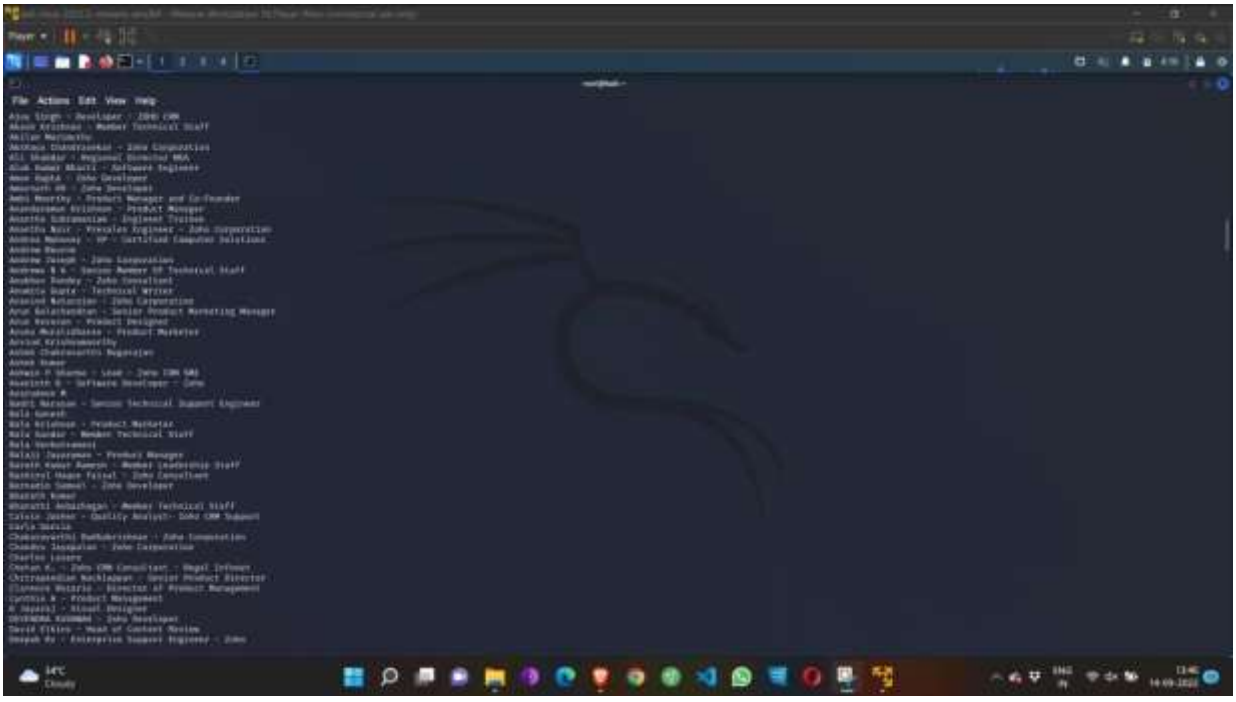
Command: theHarvester -d www.zoho.com -l 3

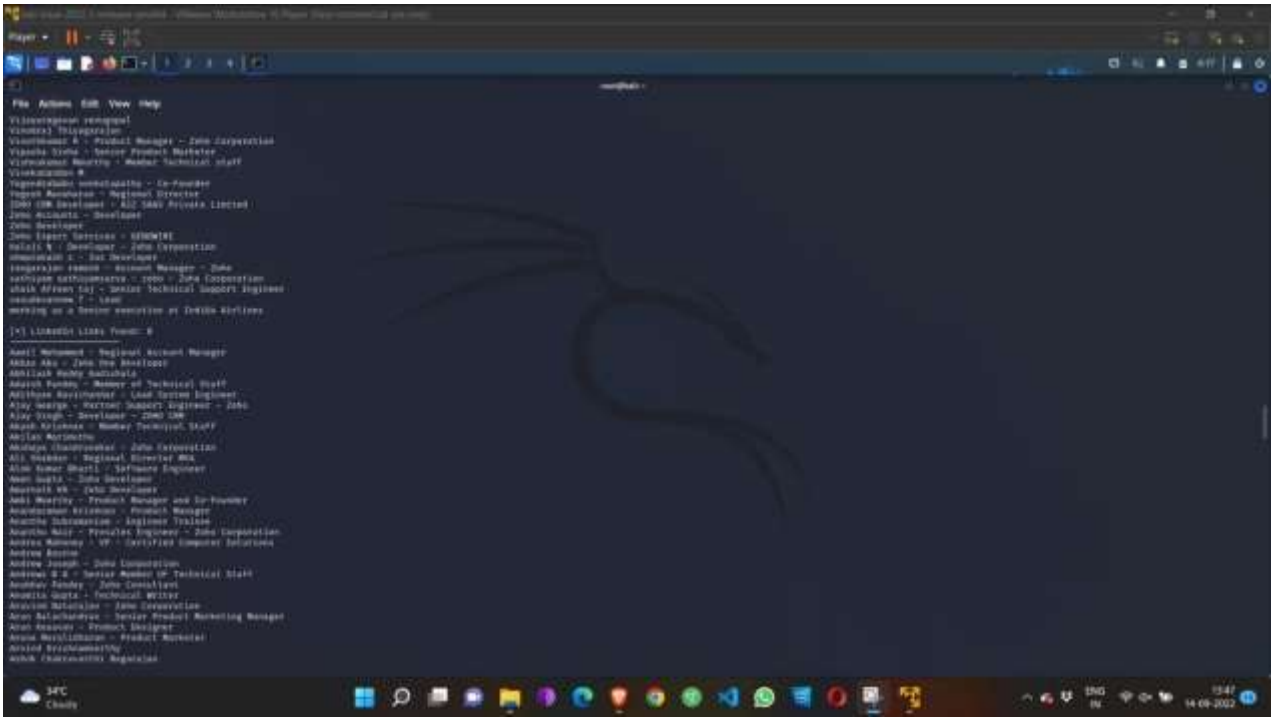


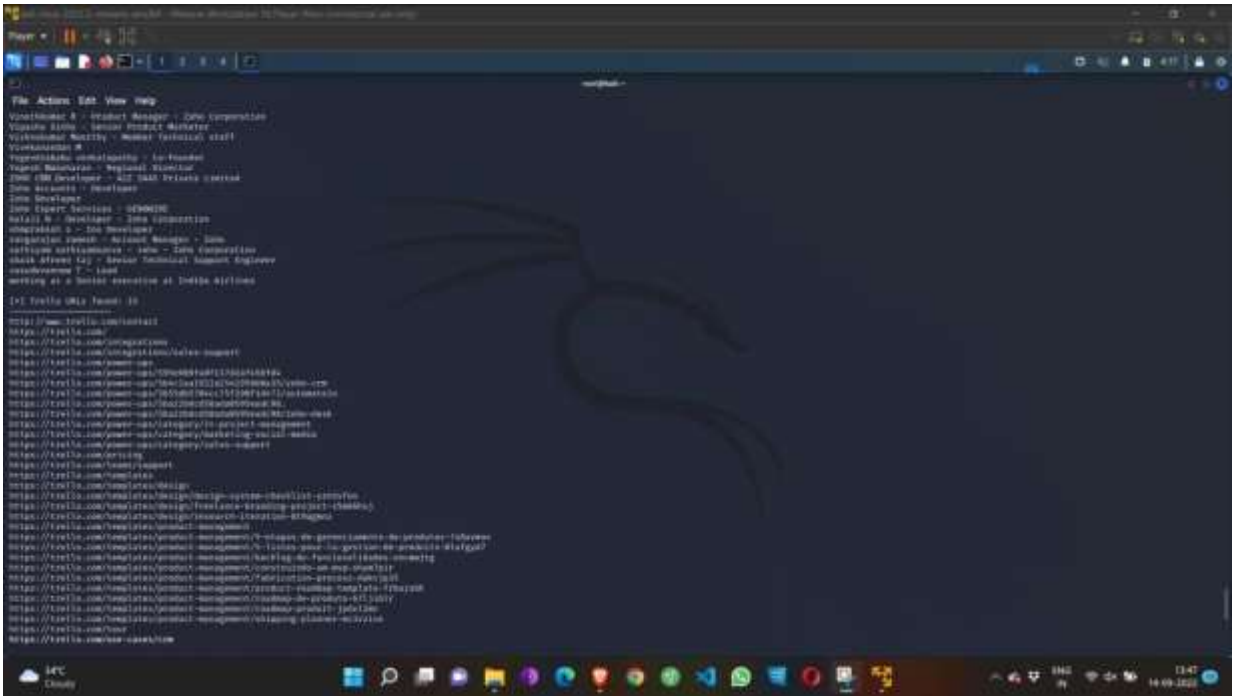
00 -b all











Step 4: run this command “**theHarvester -d www.zoho.com -l 300 -b all -f test” and** hit enter to export the result as html file and xml file

Step 5: now close the terminal and navigate the home folder and search for test file .

Out Put:

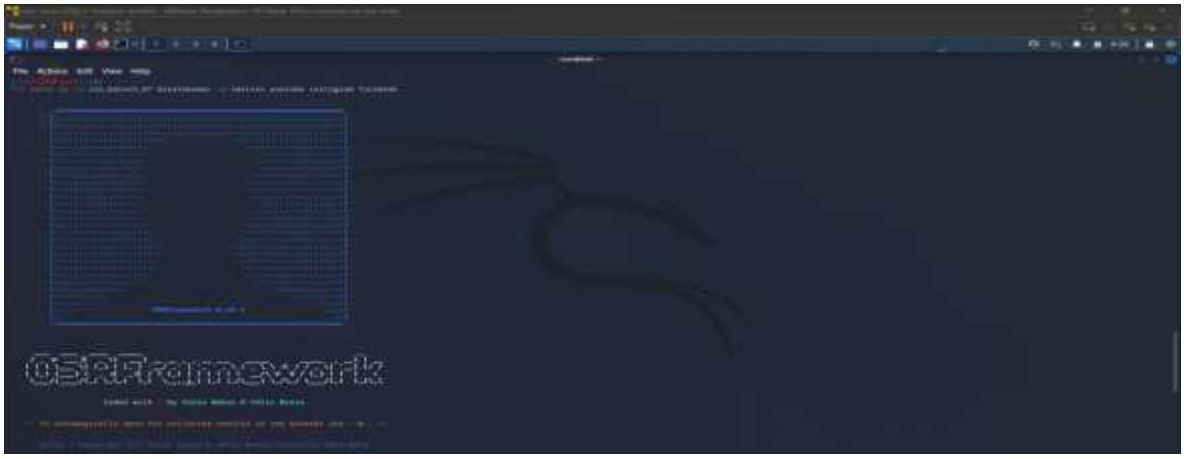
Exercise No 4- Open Source Intelligence Gathering Using OSRFramework

Aim: To Checks for the Existence of a Profile for given user details in different platforms
Procedure:

Step 1: Log into kali linux machine
Step 2: Launch a command line terminal by clicking on terminal icon from taskbar
Step 3: Usufy.py checks for the existence of a profile for given user details in different platforms

Command:

Usufy.py -n <Target username or profile name> -p twitter facebook youtube



If any error occurs Try this command: **Sudo apt-getupdate**

The usufy.py will search the user details in the mentioned platform and will provide you with the existence of the user

FIGURE. 8

Step 5: Searchfy.py checks with the existing users of a page/handlers for given details in the all social networking platforms. Type searchfy.py -q <Page Name or Handler Name> and press Enter

FIGURE. 9

Step 6: It will put out all the details who are subscribed to target social networking pages that are provided.

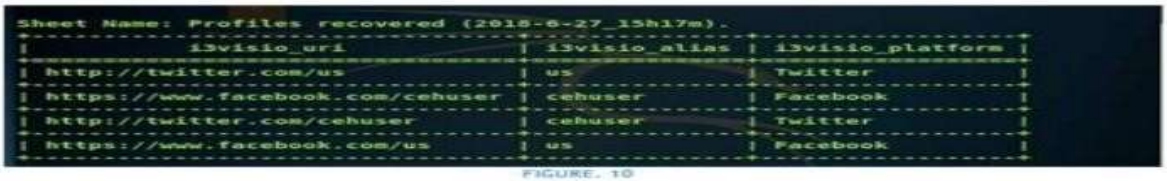
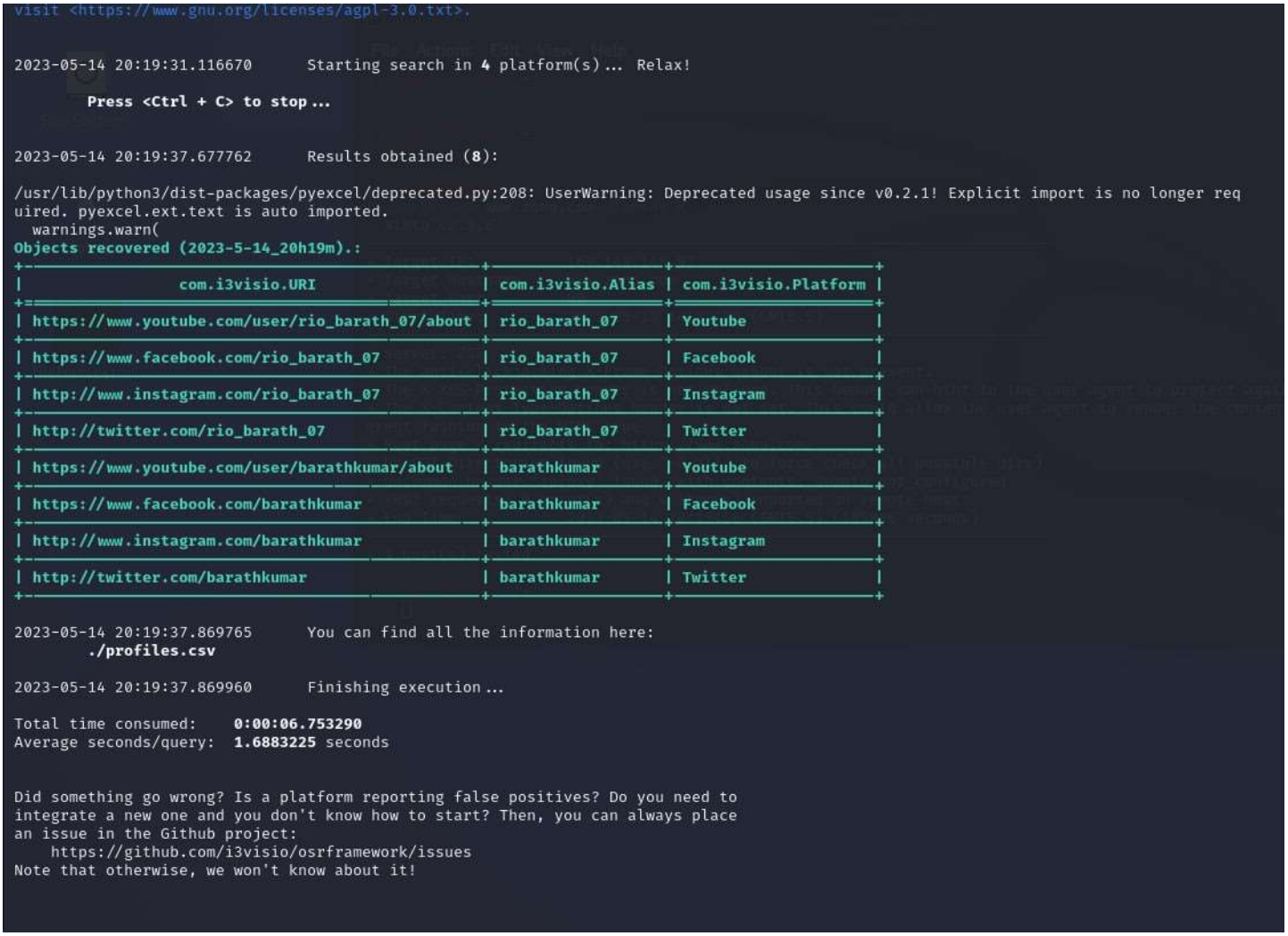


FIGURE. 10

Collect and note the information disclosed about the target

Out Put:



Exercise NO 5: Use Google and Whois for Reconnaisasance.

Aim: To find out the Whois, DNS Records and Diagonstics for particular website by using Whois search.
Procedure:

Step1: Open the WHO.is website

Step 2: Enter the website name in search bar and hit the “Enter button”. Step 3: Show you information about www.saveetha.com

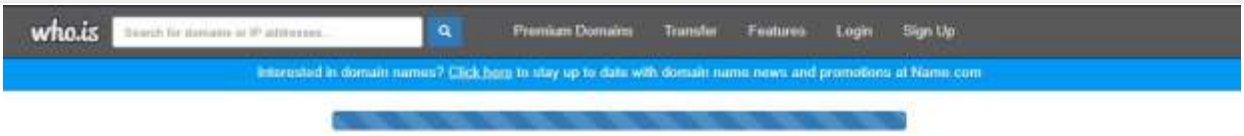
saveetha.com

DNS information

Whois | DNS Records | Diagnostics

DNS Records for saveetha.com

Hostname	Type	TTL	Priority	Content
saveetha.com	SOA	3600		ns51.domaincontrol.com dns@jomax.net 2022082301 28800 7200 604800 600
saveetha.com	NS	3600		ns51.domaincontrol.com
saveetha.com	NS	3600		ns52.domaincontrol.com
saveetha.com	A	3600		198.185.159.145
saveetha.com	A	3600		198.185.159.144
saveetha.com	MX	3600	3	alt2.aspmx.l.google.com
saveetha.com	MX	3600	1	alt1.aspmx.l.google.com
saveetha.com	MX	3600	3	alt3.aspmx.l.google.com
saveetha.com	MX	3600	3	alt4.aspmx.l.google.com
saveetha.com	MX	3600	1	aspmx.l.google.com
saveetha.com	MX	3600	2	alt2.aspmx.l.google.com
saveetha.com	MX	3600	2	alt3.aspmx.l.google.com
saveetha.com	MX	3600	1	alt4.aspmx.l.google.com
www.saveetha.com	A	3600		198.185.159.144



saveetha.com

diagnostic tools

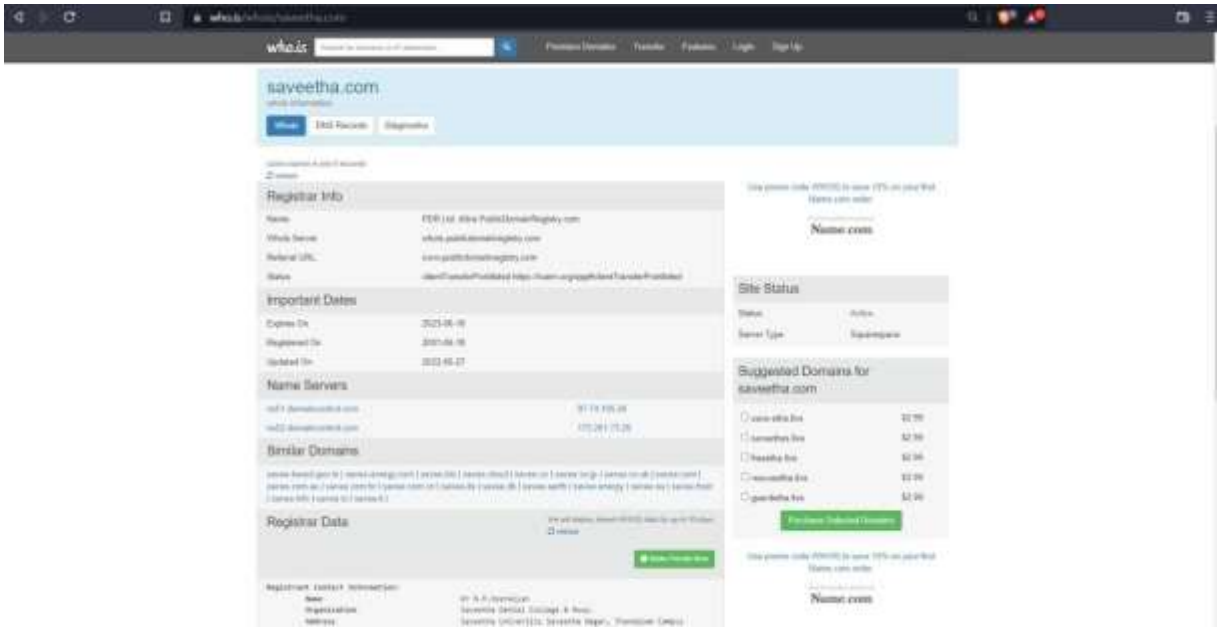
Whois | DNS Records | Diagnostics

Ping

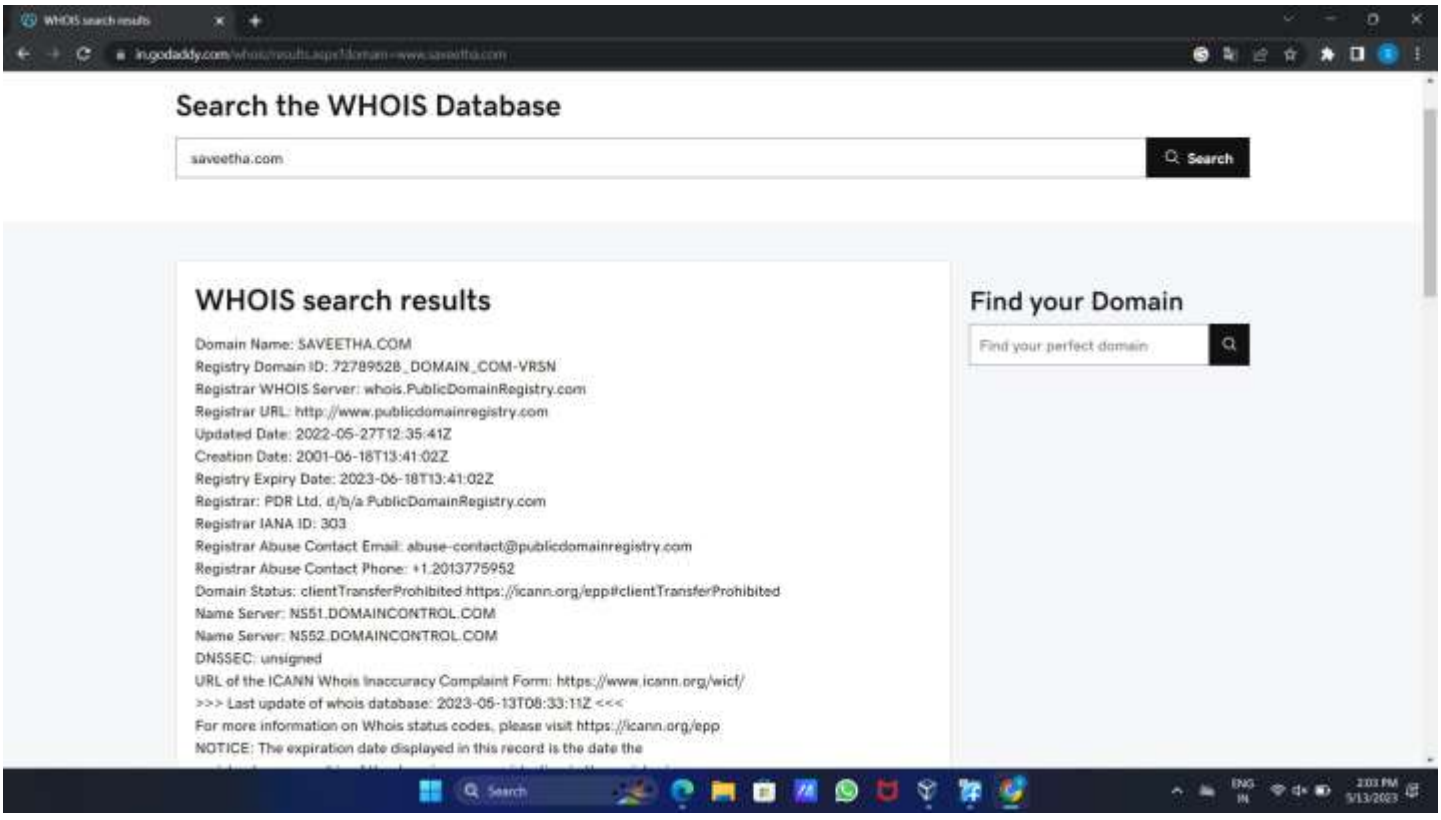
```
PING saveetha.com (198.185.159.144) 56(84) bytes of data.
64 bytes from 198.185.159.144: icmp_seq=1 ttl=47 time=8.95 ms
64 bytes from 198.185.159.144: icmp_seq=2 ttl=47 time=8.83 ms
64 bytes from 198.185.159.144: icmp_seq=3 ttl=47 time=8.85 ms
64 bytes from 198.185.159.144: icmp_seq=4 ttl=47 time=9.07 ms
64 bytes from 198.185.159.144: icmp_seq=5 ttl=47 time=9.15 ms

--- saveetha.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 8.832/8.975/9.158/0.158 ms
```

Traceroute

```
traceroute to saveetha.com (198.185.159.145), 30 hops max, 60 byte packets
 1  ip-10-0-0-14.ec2.internal (10.0.0.14)  2.160 ms  2.177 ms  2.202 ms
 2  216.182.238.135 (216.182.238.135)  11.973 ms 216.182.229.164 (216.182.229.164)  12.014 ms 216.182.229.168 (216.182.229.168)  17.582 ms
```


saveetha.com
Registrar Info
Important Dates
Name Servers
Similar Domains
Registrar Data
Site Status
Suggested Domains for saveetha.com

Out Put:

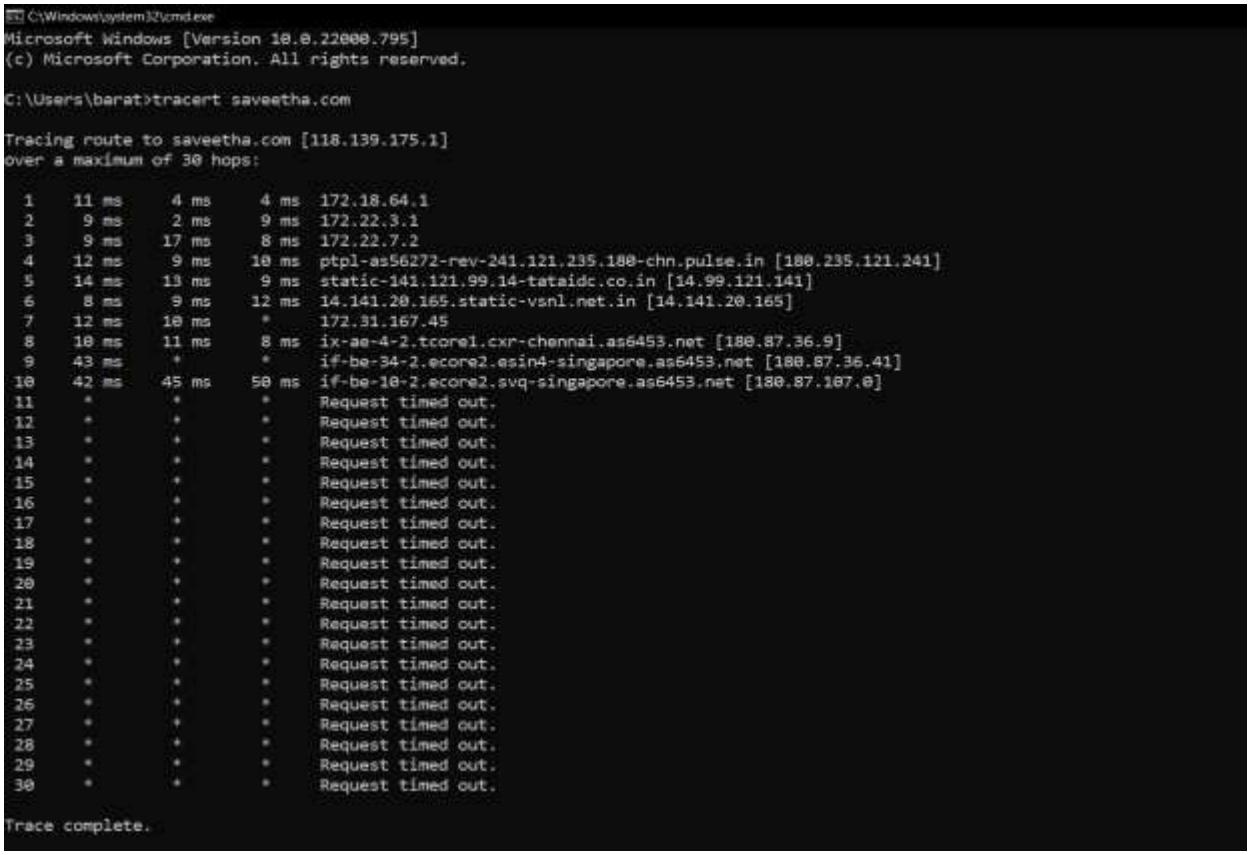

Search the WHOIS Database
saveetha.com
Search
WHOIS search results
Domain Name: SAVEETHA.COM
Registry Domain ID: 72789528_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2022-05-27T12:35:41Z
Creation Date: 2001-06-18T13:41:02Z
Registry Expiry Date: 2023-06-18T13:41:02Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-05-13T08:33:11Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
Find your Domain
Find your perfect domain

Exercise No 6: TraceRoute, ping, ifconfig, ipconfig, netstat

Aim: Using TraceRoute, ping, ifconfig(LINUX), ipconfig(WINDOWS), and netstat Command.

Procedure:

Step 1: open windows command prompt and Type tracert command and type tracert www.saveetha.com -> “Enter”



Step 2: Type ping command and type IP Address press “Enter”

```
C:\Windows\system32\cmd.exe
C:\Users\barat>ping 172.18.64.1

Pinging 172.18.64.1 with 32 bytes of data:
Reply from 172.18.64.1: bytes=32 time=7ms TTL=255
Reply from 172.18.64.1: bytes=32 time=28ms TTL=255
Reply from 172.18.64.1: bytes=32 time=34ms TTL=255
Reply from 172.18.64.1: bytes=32 time=75ms TTL=255

Ping statistics for 172.18.64.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 75ms, Average = 36ms
```

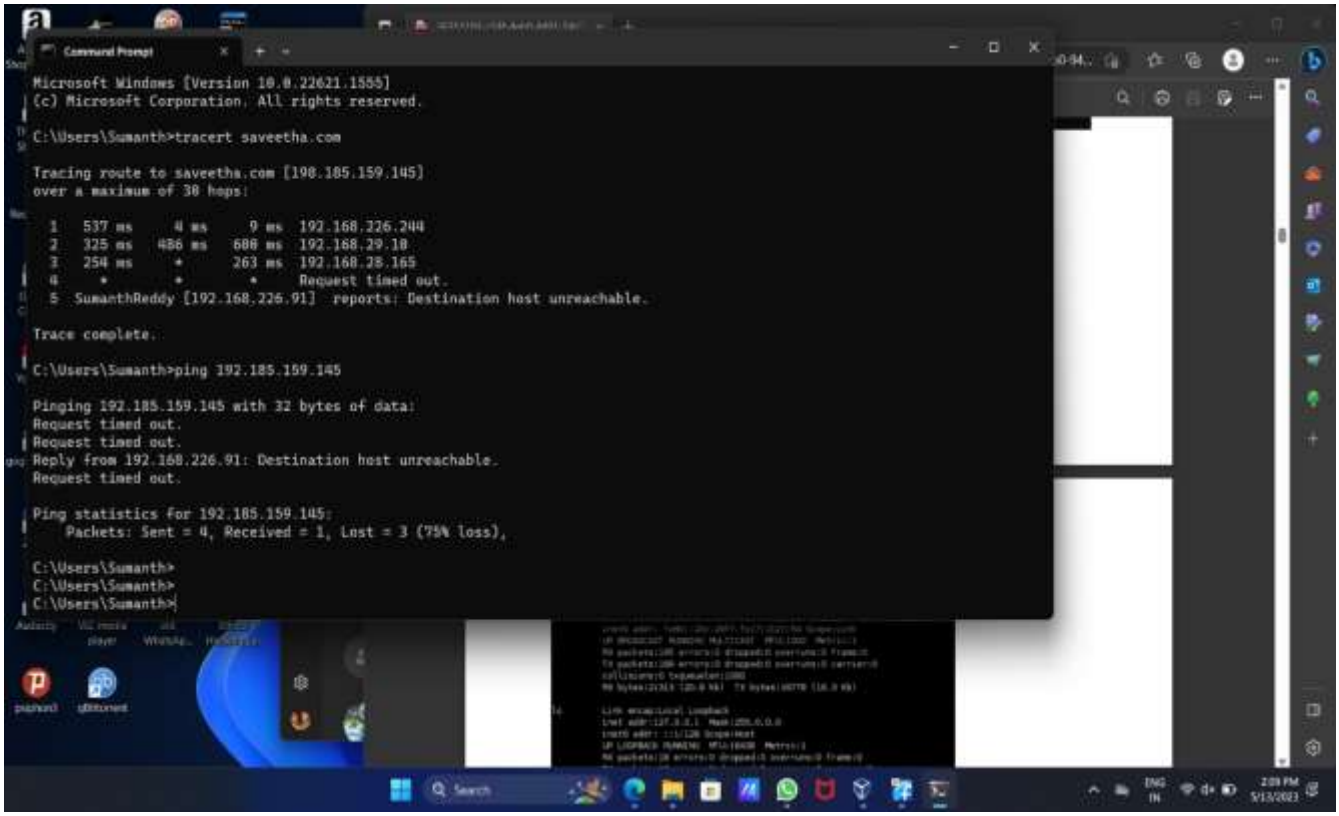
Step 3: Type ifconfig command

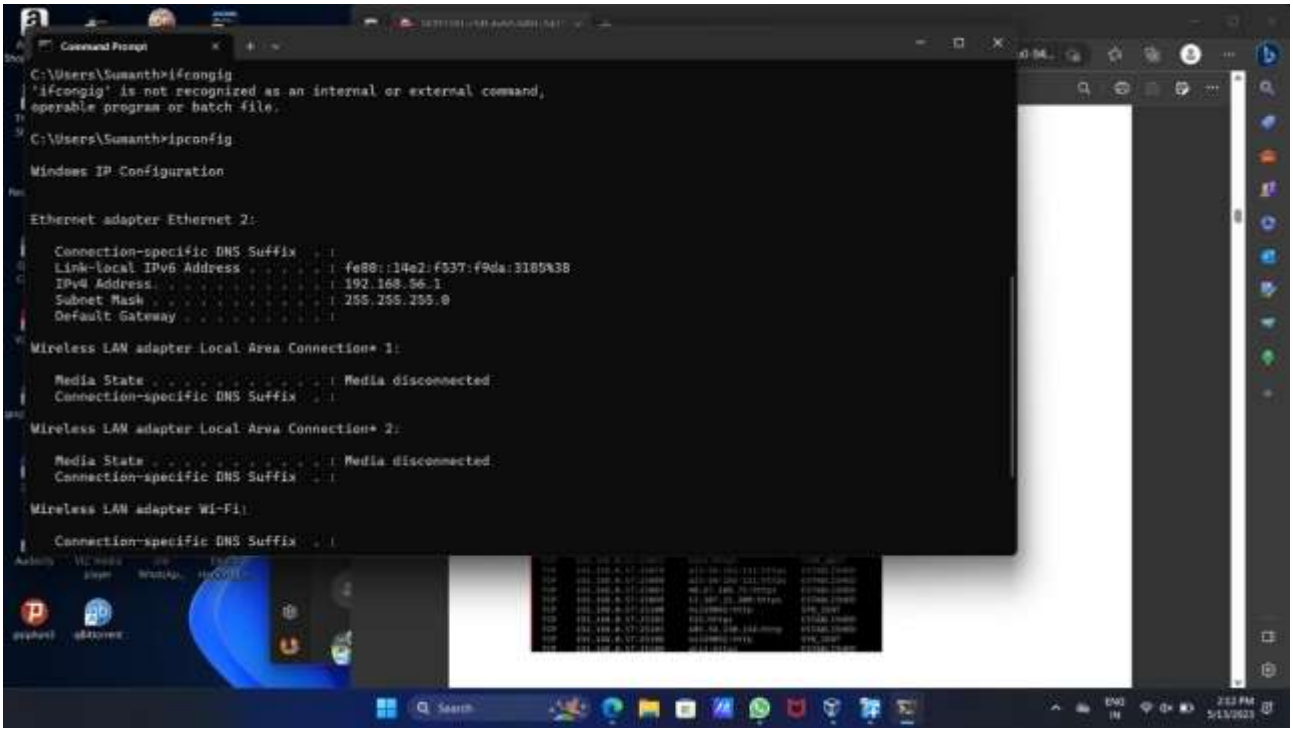
```
suse:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21313 (20.8 Kb)  TX bytes:16778 (16.3 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)
```

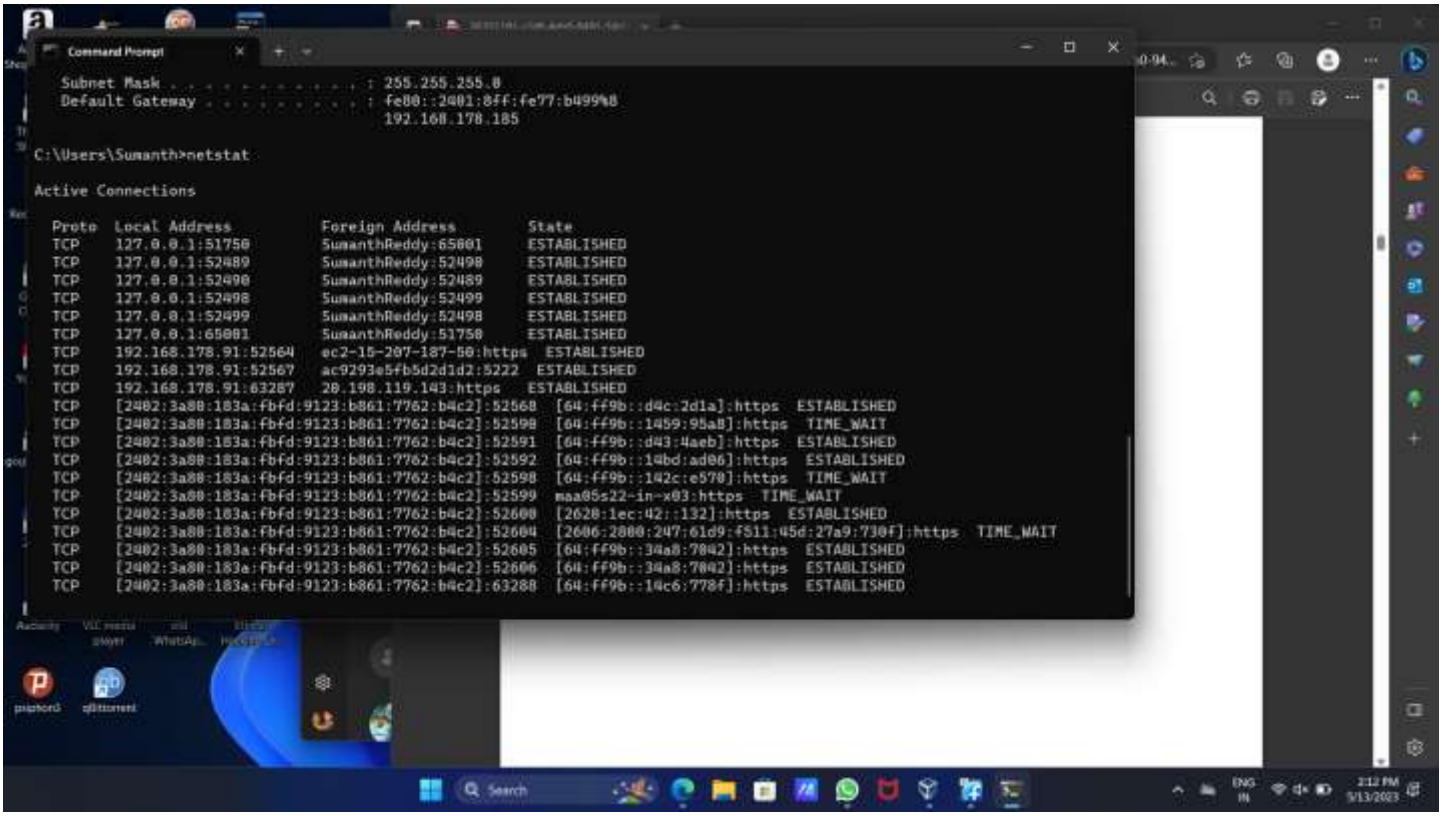
Step 4: Type netstat c

```
C:\Users\singh>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1564         DESKTOP-923RK3N:1565   ESTABLISHED
  TCP    127.0.0.1:1565         DESKTOP-923RK3N:1564   ESTABLISHED
  TCP    127.0.0.1:25104        DESKTOP-923RK3N:25105  ESTABLISHED
  TCP    127.0.0.1:25105        DESKTOP-923RK3N:25104  ESTABLISHED
  TCP    127.0.0.1:25107        DESKTOP-923RK3N:25108  ESTABLISHED
  TCP    127.0.0.1:25108        DESKTOP-923RK3N:25107  ESTABLISHED
  TCP    127.0.0.1:25112        DESKTOP-923RK3N:25113  ESTABLISHED
  TCP    127.0.0.1:25113        DESKTOP-923RK3N:25112  ESTABLISHED
  TCP    127.0.0.1:25114        DESKTOP-923RK3N:25115  ESTABLISHED
  TCP    127.0.0.1:25115        DESKTOP-923RK3N:25114  ESTABLISHED
  TCP    192.168.0.57:24938     52.230.84.217:https    ESTABLISHED
  TCP    192.168.0.57:24978     162.254.196.84:27021   ESTABLISHED
  TCP    192.168.0.57:25052     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25072     test:https             TIME_WAIT
  TCP    192.168.0.57:25078     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25080     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25083     40.67.188.75:https     ESTABLISHED
  TCP    192.168.0.57:25099     13.107.21.200:https    ESTABLISHED
  TCP    192.168.0.57:25100     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25101     155:https              ESTABLISHED
  TCP    192.168.0.57:25103     103.56.230.154:http    ESTABLISHED
  TCP    192.168.0.57:25106     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25109     ats1:https             ESTABLISHED
```

Out Put:


Command Prompt
Microsoft Windows [Version 10.0.22621.1555]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Sumanth>tracert saveetha.com
Tracing route to saveetha.com [198.185.159.145]
over a maximum of 30 hops:
1 537 ms 4 ms 9 ms 192.168.226.244
2 325 ms 486 ms 608 ms 192.168.29.10
3 254 ms * 263 ms 192.168.28.165
4 * * * Request timed out.
5 SumanthReddy [192.168.226.91] reports: Destination host unreachable.
Trace complete.
C:\Users\Sumanth>ping 192.185.159.145
Pinging 192.185.159.145 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.226.91: Destination host unreachable.
Request timed out.
Ping statistics for 192.185.159.145:
Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
C:\Users\Sumanth>
C:\Users\Sumanth>
C:\Users\Sumanth>


Command Prompt
C:\Users\Sumanth>ifcongig
'ifcongig' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Sumanth>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::14e2:f537:f9da:3185%38
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :


Command Prompt
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::2401:8ff:fe77:b499%8
192.168.178.185
C:\Users\Sumanth>netstat
Active Connections
Proto Local Address Foreign Address State
TCP 127.0.0.1:51750 SumanthReddy:65001 ESTABLISHED
TCP 127.0.0.1:52489 SumanthReddy:52498 ESTABLISHED
TCP 127.0.0.1:52490 SumanthReddy:52489 ESTABLISHED
TCP 127.0.0.1:52498 SumanthReddy:52499 ESTABLISHED
TCP 127.0.0.1:52499 SumanthReddy:52498 ESTABLISHED
TCP 127.0.0.1:65001 SumanthReddy:51750 ESTABLISHED
TCP 192.168.178.91:52564 ec2-15-207-187-50:https ESTABLISHED
TCP 192.168.178.91:52567 ac9293e5fb5d2d1d2:5222 ESTABLISHED
TCP 192.168.178.91:63287 20.198.119.143:https ESTABLISHED
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52568 [64:ff9b::d4c:2d1a]:https ESTABLISHED
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52590 [64:ff9b::1459:95a8]:https TIME_WAIT
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52591 [64:ff9b::d43:4aeb]:https ESTABLISHED
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52592 [64:ff9b::14bd:ad06]:https ESTABLISHED
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52598 [64:ff9b::142c:e570]:https TIME_WAIT
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52599 maa05s22-in-x03:https TIME_WAIT
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52600 [2620:1ec:42::132]:https ESTABLISHED
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52604 [2606:2800:247:61d9:f511:45d:27a9:730f]:https TIME_WAIT
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52605 [64:ff9b::34a8:7042]:https ESTABLISHED
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:52606 [64:ff9b::34a8:7042]:https ESTABLISHED
TCP [2402:3a80:183a:fbfd:9123:b861:7762:b4c2]:63288 [64:ff9b::14c6:778f]:https ESTABLISHED
Search
ENG
IN
2:12 PM
5/13/2023

Exercise No 7:VULNERABILITY ANALYSIS - CGI Scanning with Nikto

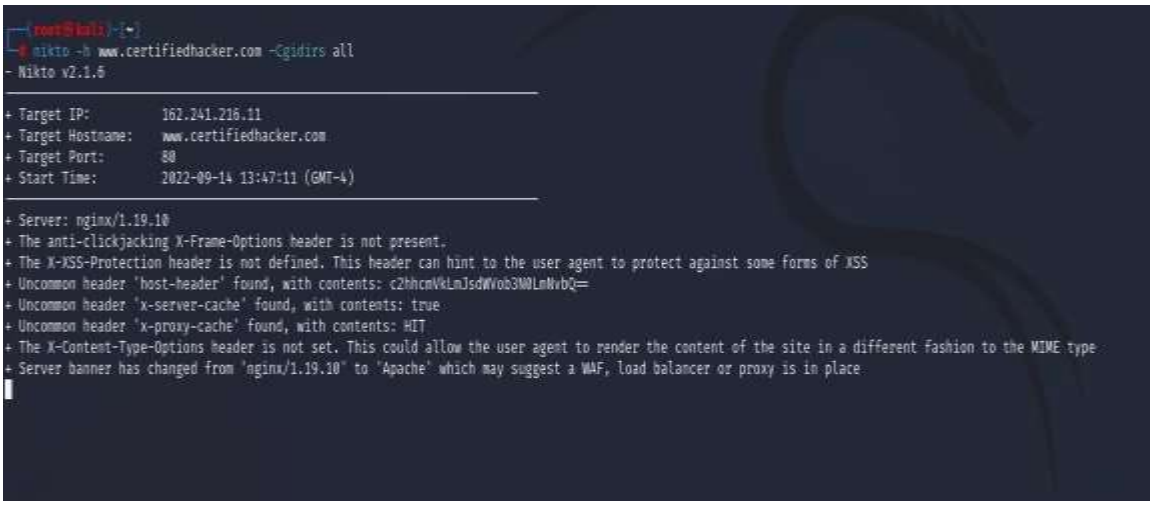
Aim:To perform vulnerability Analysis using CGI Scanning with Nikto

Procedure:

Step 1: open a terminal window and type nikto –H and press enter Step 2: Type nikto –h <website> Tuning x and press enter

Step 3: Nikto starts web server scanning with all tuning options enabled.

Step4:In the terminal window type “nikto –h <website>-Cgidirs all”and hit enter



Step 5. Nikto will scan the webserver as it looks vulnerable CGI directories. It scans the webserver and list out the directories **Out Put:**

```
nikto -h www.zoho.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          169.148.148.97
+ Target Hostname:    www.zoho.com
+ Target Port:        80
+ Start Time:         2023-05-14 20:46:15 (GMT5.5)
---------------------------------------------------------------------------
+ Server: ZGS
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.zoho.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'zproxy' found, with contents: domain_not_configured
```

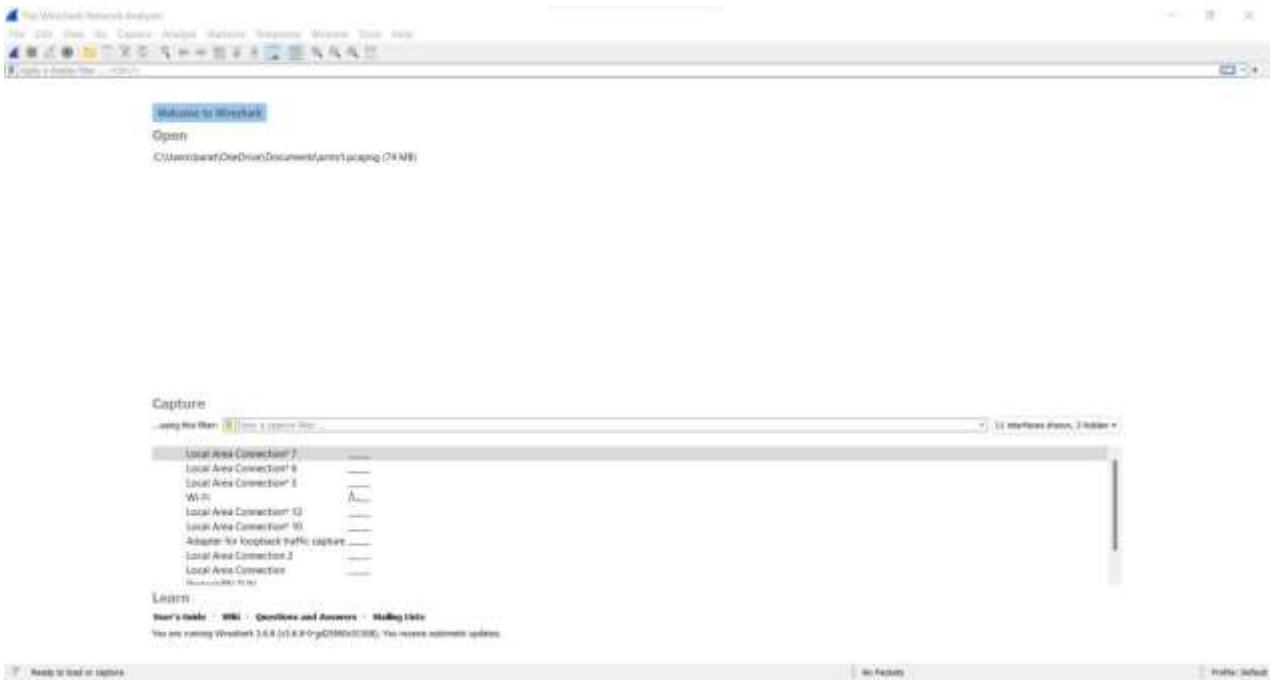
```
nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2023-05-14 20:55:18 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.certifiedhacker.com/
```

Exercise No 8: WireShark sniffer

Aim: Use WireShark sniffer to capture network traffic and analyze.

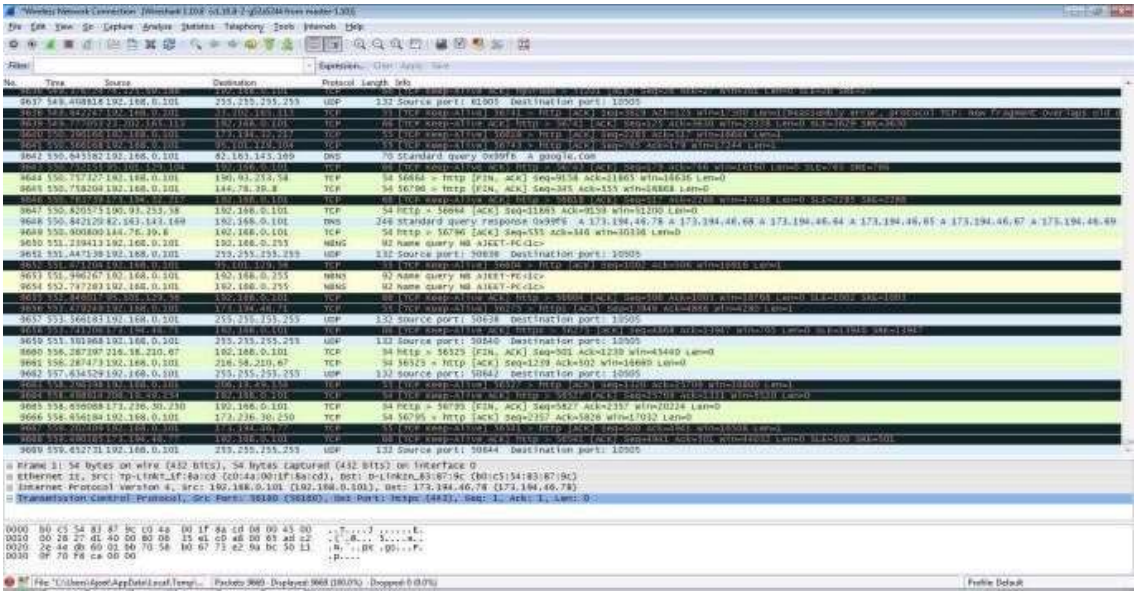
Procedure:

Step 1: Install and open WireShark .



Step 2: Go to Capture tab and select Interface option. Here Wifi connection is chosen

Step 3: The source, Destination and protocols of the packets in the Wifi network are displayed



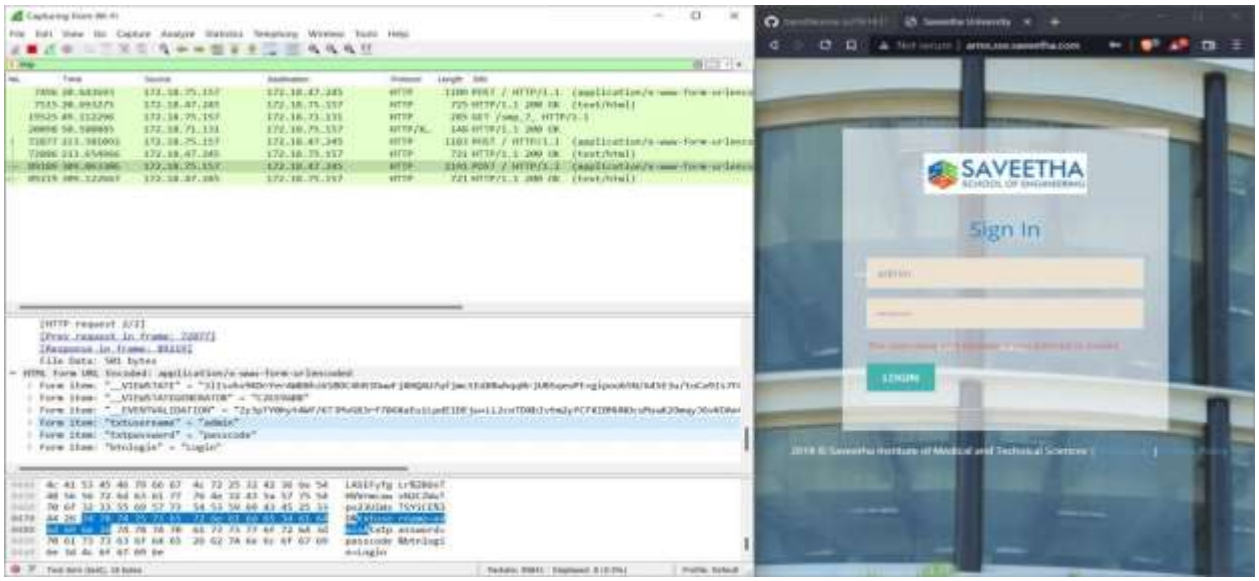
Step 4: Open a website in a new window and enter the user id and password. Register if needed.

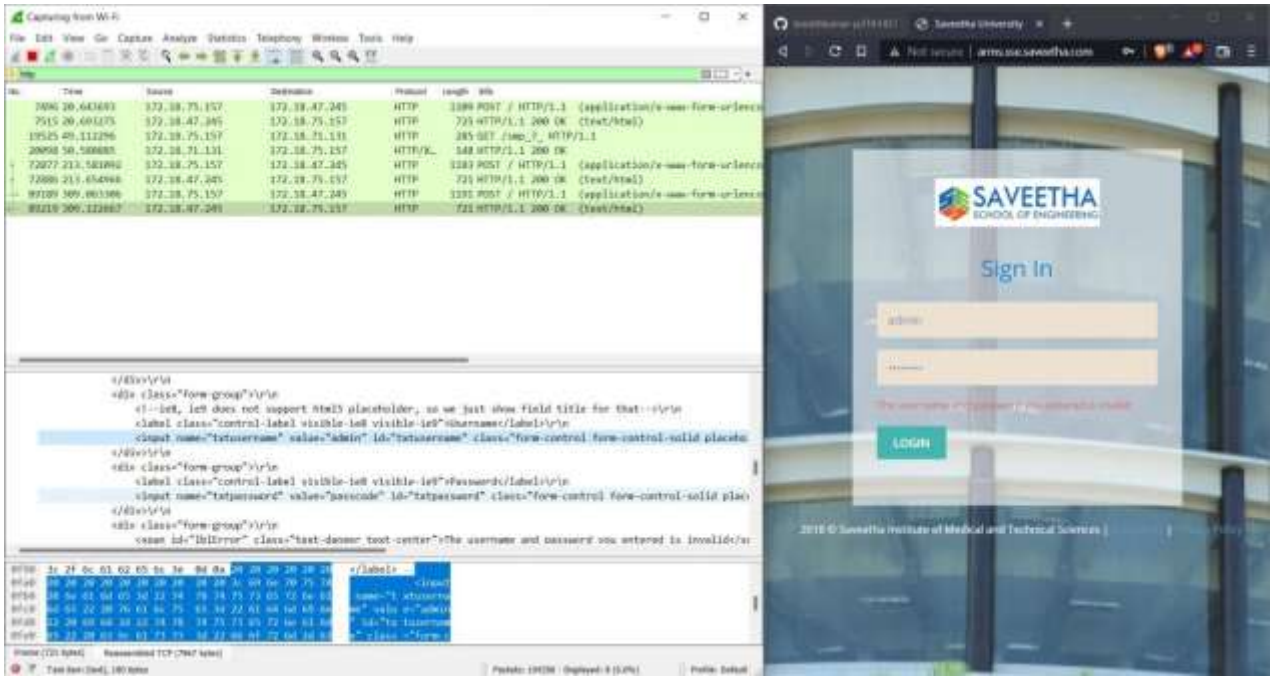
Step 5:Enter the credentials and then sign in

Step 6: The wireshark tool will keep recording the packets.

Step 7: Select filter as http to make the search easier and click on apply.

Step 9: Now stop the tool to stop recording



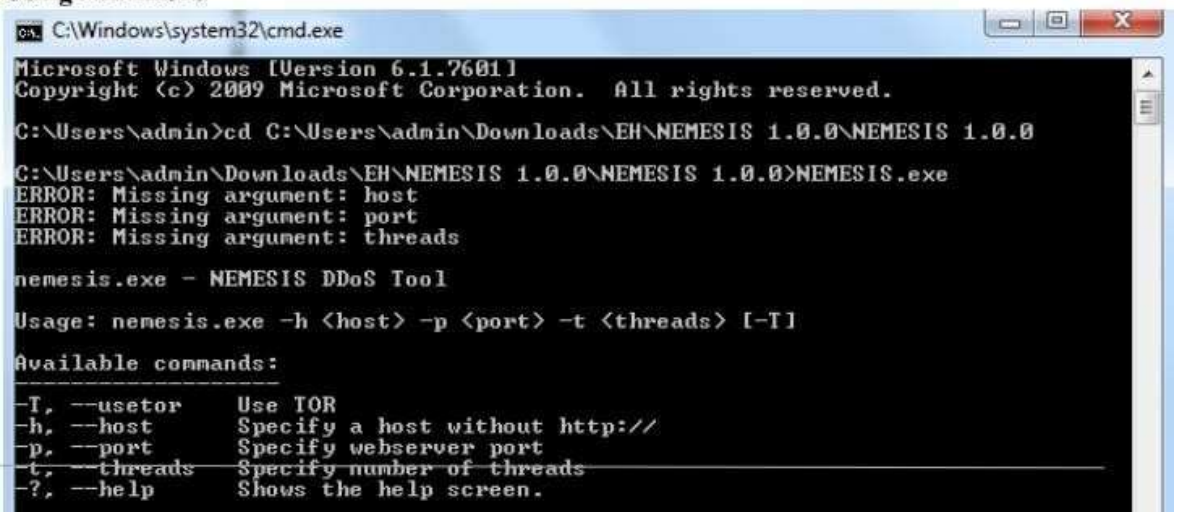


Step 10: Find the post methods for username and passwords

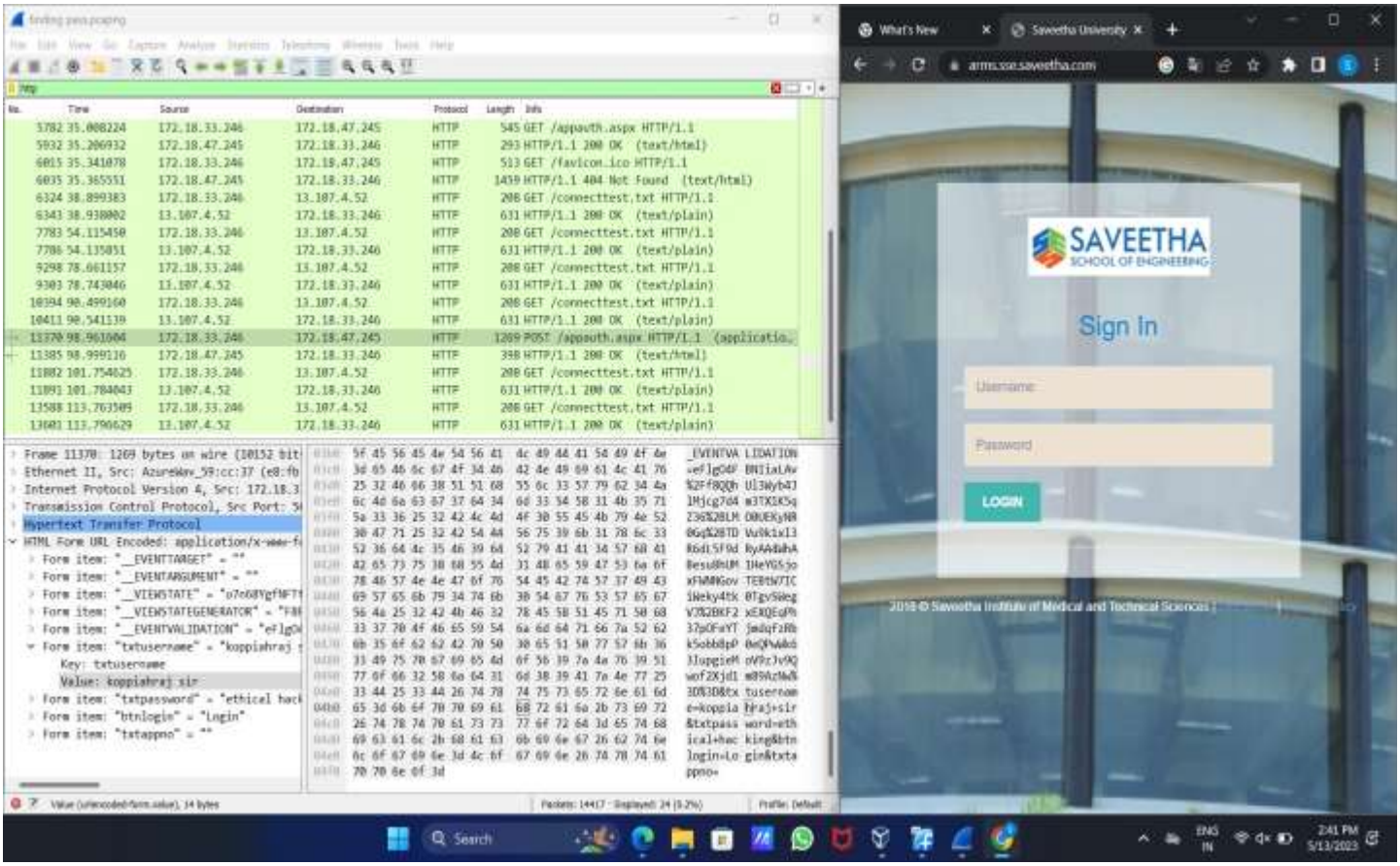
Step 11: U will see the email- id and password that you used to log in.

DOS

Using NEMESIS



Out Put:



Ex. No.9– ENUMERATION - Enumerating information from windows and Samba Host Using Enum4linux

Requirements:

- Kali linux running as an attacker machine
- Windows 7 running as virtual machine
- Admin privileges

Procedure:

1.Start the kali linux machine and open a terminal window

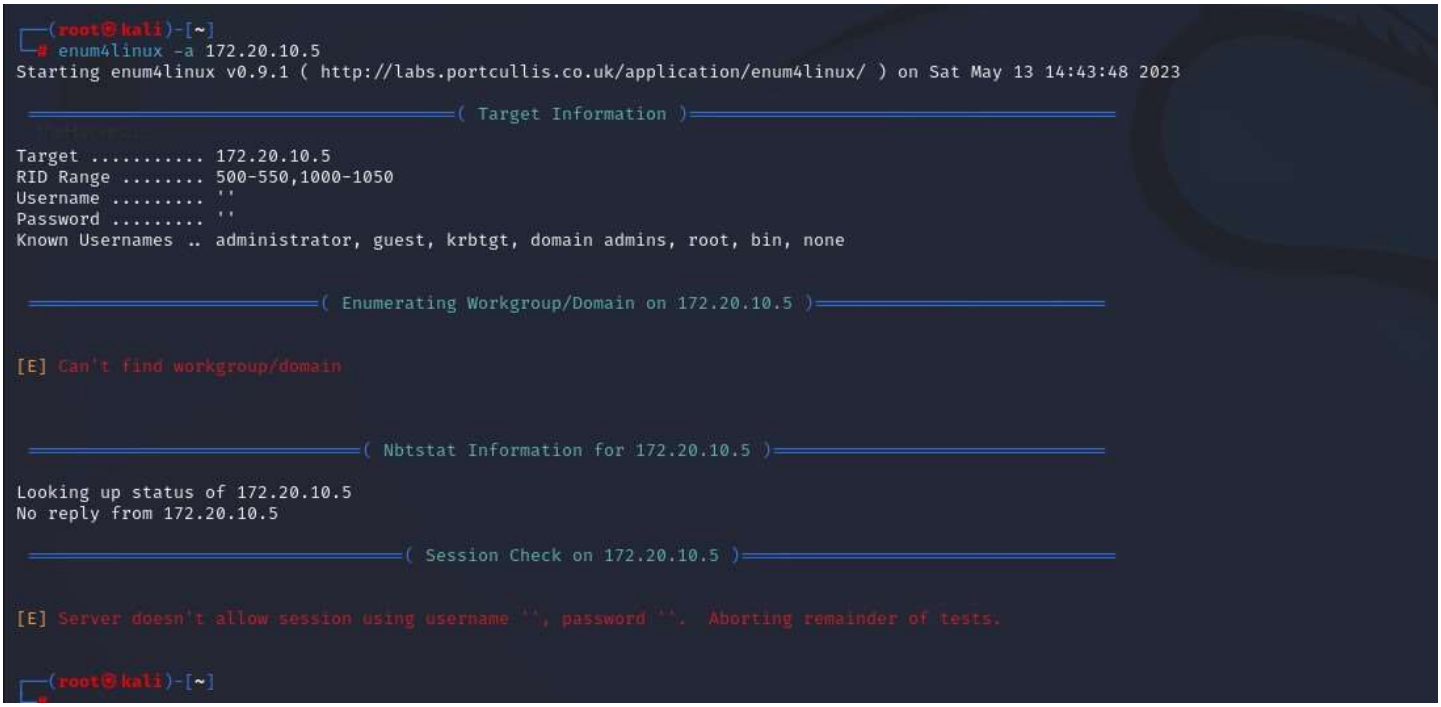
2.Type “sudo apt-get update” command

3.Now type enum4linux-h and hit enter to get help options With the help options conduct the enumeration on target machine

4.In the terminal window type enum4linux -u -p -U and hit enter to run this tool using the user list options

5.Enum4linux starts enumerating the workgroups/domain names first and display the results

6.To enumerate all the information Use this command enum4linux -a



EX.NO: 10 **DATE: BATCH FILE EXECUTION**

AIM: To create a Windows batch file.

PROCEDURE:

Step 1 : Open a text file, such as a Notepad or WordPad document

Step 2 : Add your commands, starting **with @echo [off],** followed by, each in a new line, **title [title of your batch script], echo [first line],** and **pause.**

Step 3 : Save your file with the file extension **BAT,** for example, **test.bat.**

Step 4 : To run your batch file, **double-click the BAT file** you just created.

Step 5 : To edit your batch file**, right-click the BAT file** and select **Edit**.

And here's the corresponding command window for the example above:

1.Create a New Text Document

A batch file simplifies repeatable computer tasks using the Windows command prompt.

Below is an example of a batch file responsible for displaying some text in your command prompt.

Create a new BAT file by right-clicking an empty space within a directory and selecting **New, then Text Document**.

1.CODE:

Double-click this **New Text Document** to open your default text editor. Copy and paste the following code into your text entry.

>> @echo off

>> echo hello

>> Pause

>> echo This is new

>> echo this is second one

>> pause

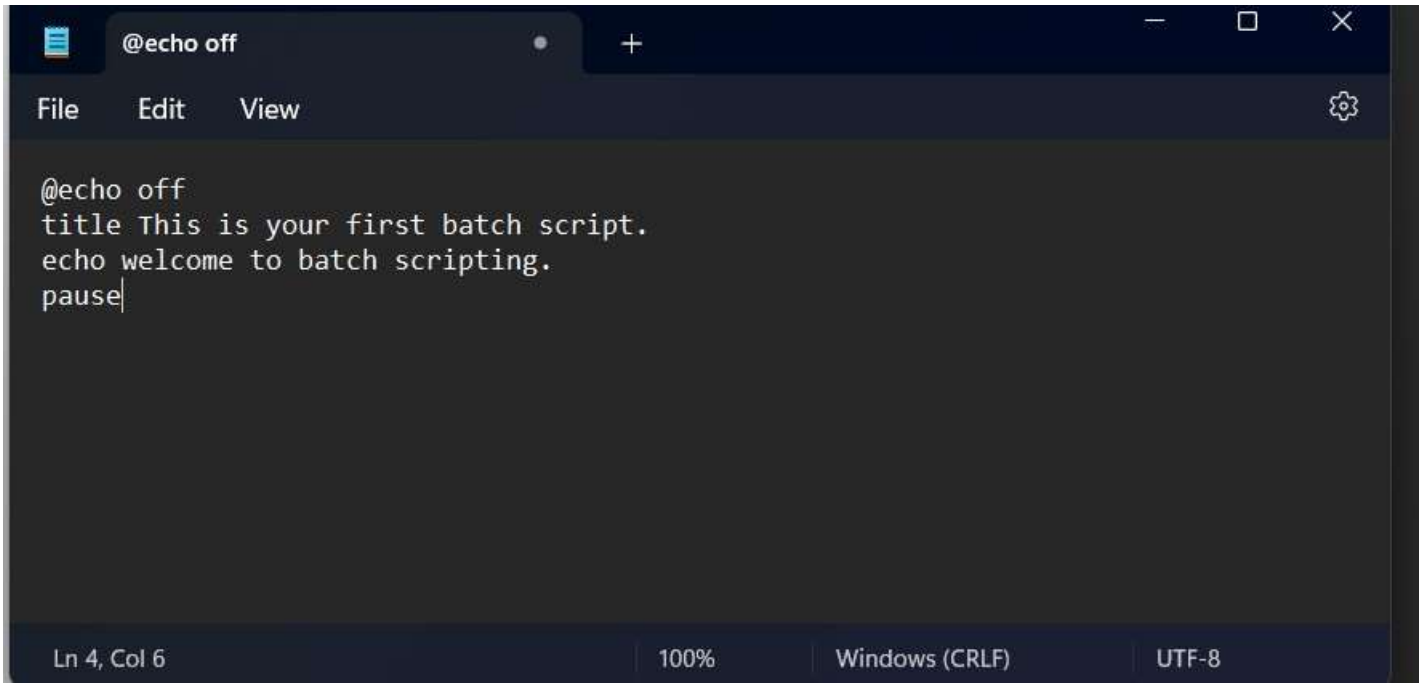
1. TO SAVE a BAT File

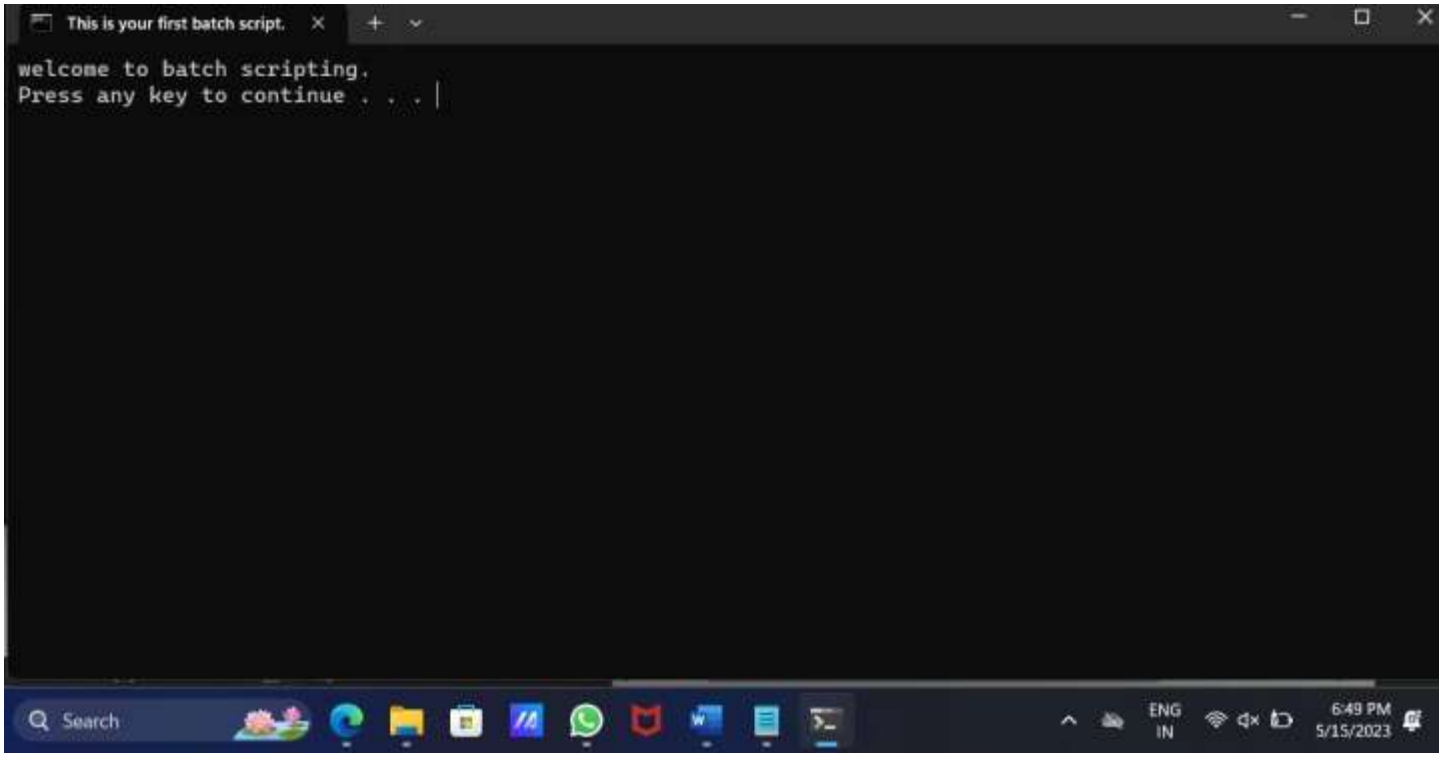
The above script echoes back the text "Welcome to batch scripting!" Save your file by heading to **File > Save As,** and then name your file what you'd like. End your file name with the added **BAT** extension, for example **test.bat,** and click **OK**. This will finalize the batch process. Now, double-click on your newly created batch file to activate it.

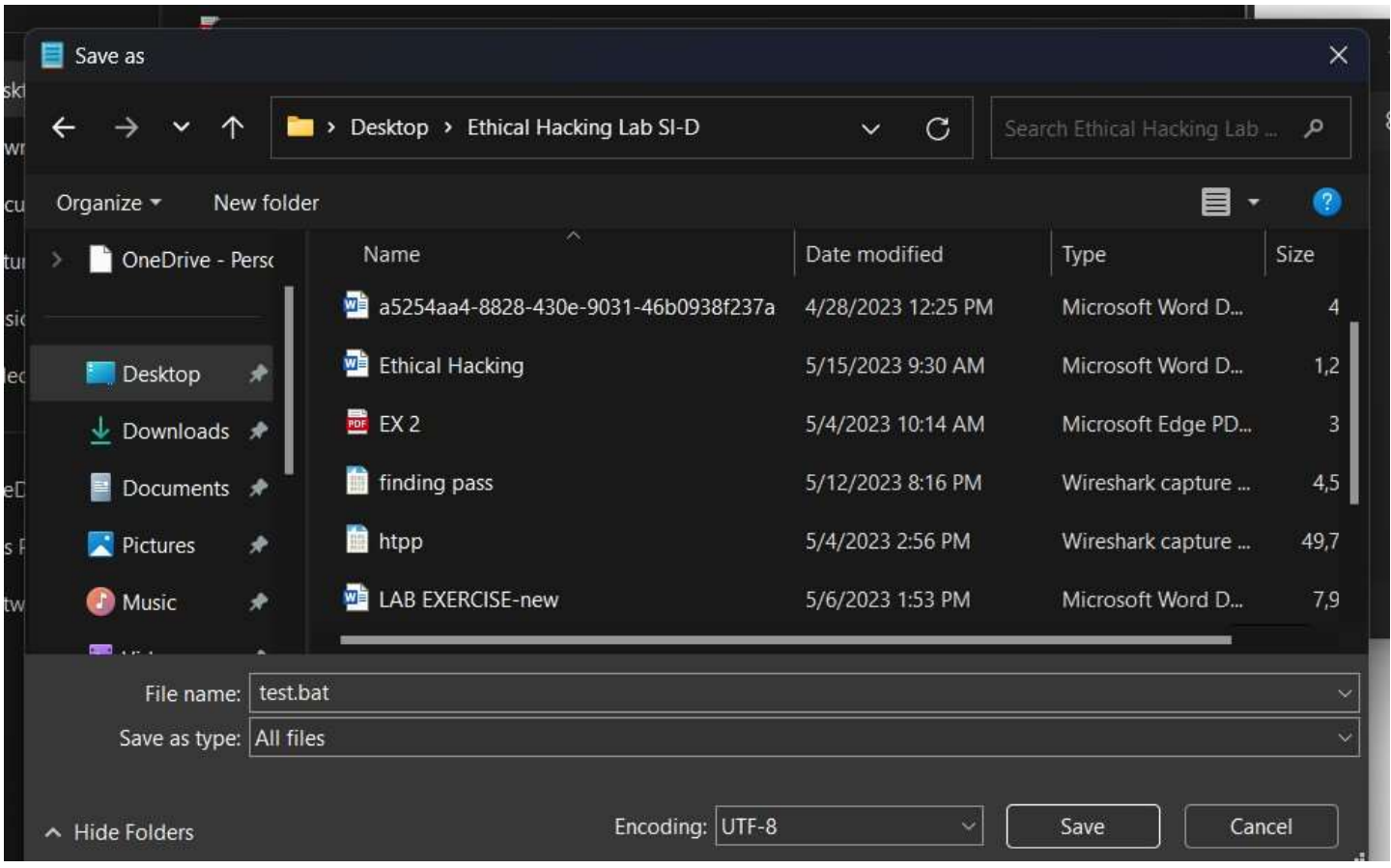
2.To RUN as BAT File

Once you'd saved your file, all you need to do is **double-click your BAT file**. Instantly, your web pages will open. If you'd like, you can place this file on your desktop. This will allow you to access all of your favorite websites at once.

OUT PUT:




This is your first batch script.
welcome to batch scripting.
Press any key to continue . . .
Search
ENG
IN
6:49 PM
5/15/2023


Save as
Desktop › Ethical Hacking Lab SI-D
Search Ethical Hacking Lab ...
Organize
New folder
OneDrive - Perso
Desktop
Downloads
Documents
Pictures
Music
Name
Date modified
Type
Size
a5254aa4-8828-430e-9031-46b0938f237a
4/28/2023 12:25 PM
Microsoft Word D...
4
Ethical Hacking
5/15/2023 9:30 AM
Microsoft Word D...
1,2
EX 2
5/4/2023 10:14 AM
Microsoft Edge PD...
3
finding pass
5/12/2023 8:16 PM
Wireshark capture ...
4,5
htpp
5/4/2023 2:56 PM
Wireshark capture ...
49,7
LAB EXERCISE-new
5/6/2023 1:53 PM
Microsoft Word D...
7,9
File name: test.bat
Save as type: All files
Hide Folders
Encoding: UTF-8
Save
Cancel

RESULT:

Thus the Creation and execution of BATCH FILE was successfully completed.